حملة - المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

الأمان الرقمي بين الشباب الفلسطيني في الداخل

دراسة حول التهديدات والتحديات في ظل الحرب على غزة

آب 2024

حملة – المركز العربي لتطوير الإعلام الاجتماعي

الأمان الرقمي بين الشباب الفلسطيني في الداخل:
دراسة حول التهديدات والتحديات في ظل الحرب على غزة

المؤلف: د. سعيد أبو معلا

تنفيذ استطلاع : داتا نيو فيجن

تحرير اكاديمي : ايناس خطيب

تدقيق النسخة العربية: مروى حنا

تصميم : أمل شوفاني

رُخّص هذا الإصدار بموجب الرّخصة الدّولية: نَسب المُصنّف -غير تجاري- منع الاشتقاق 4.0 دولي

للاطلاع على نسخة من الرّخصة،يُرجى زيارة الرابط التّالي:
https://creativecommons.org/licenses/by-nc-nd/4.0 Comment end

للتواصل معنا:

البريد الإلكترونيّ: info@7amleh.org

الموقع الإلكترونيّ: www.7amleh.org

الهاتف: 774020670 (0) 972+

صفحاتنا على وسائل التواصل الاجتماعيّ: **7amleh**

الفهرس

ملخّص تنفيذيّ 4

الباب الأوّل 7

مقدّمة عامّة 7

الباب الثاني 12

منهجية الدراسة 12

الباب الثالث 14

نتائج الدراسة التحليلية 14

ملخص ونقاش النتائج العامة 38

ملخص تنفيذي

تسلط هذه الدراسة الضوء على مشهد الأمان الرقمي بين الشباب العربي الفلسطيني ممن يحملون الجنسية الإسرائيلية، من خلال تقفي تجارب مستخدمي شبكة الإنترنت الفلسطينيّين، جاءت هذه الدراسة في مرحلة غاية في الحساسية والاضطراب والتحوّل. بغية استخلاص استنتاجات ذات مصداقية استخدمت الدراسة طريقتين لجمع البيانات، هما: المجموعات البؤرية (4 مجموعات ضمت 23 مشاركًا/ةً)، والمسح الميداني (استطلاع رأي شارك فيه 409 مستطلَعين/ات)، إلى جانب مراجعة الأدبيات التي تناولت موضوعي الأمان الرقمي والحقوق الرقمية. تراوحت الأعمار المشاركة في الاستطلاع بين 15 و30 عامًا، وقد تم تنفيذ الدراسة خلال النصف الأول من العام 2024.

احتوت استمارة الاستطلاع على 27 سؤالًا، وُزعت على خمسة محاور هي: خصائص المستطلَعين/ات؛ خصائص استخدامات شبكة الإنترنت لدى المستطلَعين/ات؛ مدى معرفة "الأمان الرقمي" ومدى إدراك المخاطر الرقمية، أنواع الهجمات والاعتداءات الرقمية ومدى التعرض لها؛ المساءلة والتحقيق من جهات أمنية إسرائيلية وجهات اجتماعية وسياسية لأسباب لها علاقة بالنشاط الرقمي؛ أثر سياسات منصات التواصل الاجتماعي على نشاط الشباب الفلسطيني منذ بدء الحرب على قطاع غزة. بعد تحليل بيانات الاستطلاع خلصت الدراسة إلى الآتي:

- **81% من المستطلَعين/ات يستخدمون الإنترنت في المنزل.**
- **48% من المستطلَعين/ات يقضون من 4 إلى 9 ساعات يومية باستخدام الإنترنت.**
- **يستخدم المستطلَعون/ات مجموعة كبيرة من التطبيقات والشبكات الاجتماعية أبرزها: "واتس اب 86%" و"فيس بوك" 83% و"انستغرام" 84% و"تيك توك" 60% و"تلغرام" 40% و"سناب شات" 30% و"شبكة إكس" (تويتر سابقًا) 18%.**
- **67% من المستطلَعين/ات صرّحوا أنهم يعرفون أو سمعوا عن برامج تجسس الأجهزة الإلكترونية المرتبطة بالشبكة.**
- **55% مِن مَن يعرفون عن برامج التجسس مصدر معلوماتهم القراءة أو المشاهدة حول هذه البرامج من "مجلات أو مواقع إلكترونية".**
- **55% من المستطلَعين/ات لم يغيّروا كلمة المرور إطلاقًا.**
- **65% من المستطلَعين/ات يفعّلون إعدادات الأمان.**
- **83% من المستطلعين/ات نادرًا ما يصادقون على طلبات صداقة من أشخاص مجهولين، ومن تبقى يصادقون بوتيرة متفاوتة.**
- **55% من المستطلَعين/ات نادرًا ما يشاركون صورًا وأمورًا شخصيّة على الشبكة.**
- **69% من المستطلَعين/ات لا يستخدمون برامج الحماية.**

- **42%** من المستطلَعين/ات لا يرون أن برامج الحماية تعود عليهم بالفائدة.
- **27%** من المستطلَعين/ات لا يثقون بمصادر برامج الحماية.
- **79%** من المستطلَعين/ات لا يستخدمون أي حماية رقميّة.
- **55%** من المستطلَعين/ات يتجاهلون رسائل مجهولة المصدر.
- **71%** من المستطلَعين/ات يستخدمون خاصية تحديد المواقع الجغرافية.
- **10%** من المستطلَعين/ات تعرضوا لهجوم أو اعتداء رقميّين.
- **53%** من المستطلَعين/ات تجاهلوا الهجوم والاعتداء.
- **74%** من المستطلَعين/ات قالوا إنهم تعرضوا لهجوم أو اعتداء لفظي (**47%** غرباء و**37%** معارف عربًا).
- **39%** من المستطلَعين/ات اختاروا التجاهل ولم يتوجهوا لأي طرف لحل المشكلة.
- **42%** من المستطلَعين/ات تعرضوا لهجوم او اعتداء من نوع "انتحال الشخصية".
- **55%** من المستطلَعين/ات تعرضوا لهجوم أو اعتداء من نوع "التحرش" و "التصيد الاحتيالي".
- **10%** من المستطلَعين/ات تعرضوا شخصيًّا أو يعرفون شخصًا تعرض للمساءلة والتحقيق من السلطات الإسرائيليّة.
- **6%** من المستطلَعين/ات تعرضوا لضغوطات من دوائر اجتماعية لحذف منشوراتهم.
- **70%** من المستطلَعين/ات قالوا إنهم يمارسون رقابة ذاتية على نشاطهم الرقميّ.
- **93%** من المستطلَعين/ات قالوا إنهم لم يتعرضوا لأي تقييد أو حذف من قبل شبكات التواصل الاجتماعي.

بجانب نتائج المسح الميداني، توصلت الدراسة من خلال نقاشات المجموعات البؤرية إلى عدة استنتاجات، كان من أبرزها ما يلي:

- **حذف مئات الأصدقاء**، منذ بدء الحرب على غزة حذف/ت المشاركات/ين في المجموعات البؤرية مئات الأصدقاء (أصدقاء الأصدقاء، معارف، زملاء يهود إسرائيليين) من حساباتهن/م على شبكات التواصل الاجتماعي.

- **الإحساس بعدم الأمان**، بدأ التصاعد في هذا الإحساس منذ هبة أيّار 2021، وتصاعد تصاعدًا حادًّا منذ بدء الحرب على غزة، وعزت المشاركات/ين هذا الإحساس للملاحقة الأمنية والقمع العنيف الذي تمارسه السلطات الإسرائيلية الأمنية والقضائية تجاه الناشطات/ين أو حتى الشباب غير المنخرطين في النشاط السياسي والاجتماعي.

- **التعرض للهجوم**، جزء لا بأس به من المشاركات/ين قالوا إنهم تعرضوا للهجوم أو "التطفل" من جهات مختلفة، منها على سبيل المثال، الأمنية والسياسية والاجتماعية والدينية. وصفت المشاركات/ين أن من وقفوا خلف الهجوم عملوا بتناغم.

- **فقدان الثقة**، التناغم بين أطراف الهجوم، وفي بعض الأحيان التواطؤ بين حكومة إسرائيل وأجهزتها وبين منصات التواصل الاجتماعي، أدى إلى فقدان الثقة لدى المشاركات/ين في الجهات التي يُفترض أن توفر لهن/م الحماية والحلول.

- **كيّ الوعي**، استطاعت حكومة إسرائيل متمثلة في أجهزتها الأمنية والقضائية أن تعزز من حالة القمع الذاتي، بواسطة ملاحقة واعتقال شخصيات معروفة بسبب منشورات إنسانية أو دينية على منصات التواصل الاجتماعي. وهذا ما دفع بعض الشخصيات السياسية الفلسطينية في الداخل مطالبة الجمهور بعدم التفاعل على منصات التواصل الاجتماعي والتحلي "بضبط النفس".

- **فقدان الأمل**، هذا الشعور السائد بين الناشطات في مجال حقوق الإنسان، بسبب تجارب الملاحقة والتهجمات والاعتداءات التي عشنها على منصات التواصل الاجتماعي وعلى أرض الواقع. فقدان الأمل من أي تغيير سياسي أو اجتماعي.

- **تراجع النشاط الرقمي**، حالة العجز الرقميّة والخوف التي تعيشها الناشطات في مجال حقوق الإنسان أدت إلى تراجع نشاطهن الرقمي، والاكتفاء بالتزود بالأخبار.

- **عدم جهوزية المؤسسات الوطنية والحقوقية**، منذ بدء الحرب على قطاع غزة (2023) ومن قبلها هبة أيّار (2021) لم تكن المؤسسات الوطنية والحقوقية والأهلية ذات جهوزية توفر الحماية والأمان الرقميان لموظفيها وكل من يتلقى خدماتها.

تظهر المعطيات أن المستخدمين يعيشون حالة من الخوف والقلق تظهر بالممارسات، علاوة على شعورهم بفقدان الثقة الذي تُرجم إلى لامبالاة وتجاهل تام لكل المخاطر المحدقة بهم. فضلًا عن عدم جهوزية المؤسسات على اختلاف أنواعها لتوفير المعرفة الرقمية والأمان الرقمي لموظفيها ومستخدميها.

الباب الأول

مقدمة عامة وإطار نظري

تمارس الحكومة الإسرائيلية أنماطًا من سياسات السيطرة والرقابة والقمع على الفلسطينيين في إسرائيل منذ النكبة، وإن كان بأشكال وأدوات مختلفة تغيرت على مر السنين بحسب الأحداث والوقائع. تعاملت الحكومة الإسرائيلية ومؤسساتها مع الفلسطينيّين المواطنين فيها على أنهم غير يهود وعلى أنهم مجموعة من الأقليّات المنعزلة، وقد أسهمت هذه التقسيمات في تعزيز السيطرة على الفلسطينيين في إسرائيل وضبطهم. أفشلت أحداث يوم الأرض والانتفاضة الأولى والثانية وما تلاها من من أحداث وحراكات وهبات شعبية هذه التجزئة إلى جانب إعادة اللُحمة مع باقي أجزاء الشعب الفلسطيني. وقد أطلقت غانم وصف "وضعية العتبة" على وضعية الفلسطينيين في إسرائيل التي نتجت عن النكبة وسياسات الحكومات الإسرائيلية المتراكمة؛ فهم يعيشون ويعملون- مدنيا وسياسيا- على عتبة النظام الإسرائيلي من جهة وعلى عتبة المركز السياسي والوطني الفلسطيني لأنهم جزء من هذا الشعب.[1] تحاول الحكومات الإسرائيلية استغلال هذه الوضعية لتبرير سياسات السيطرة والرقابة والقمع المعززة بالقوانين وباستخدام آليات وأدوات كلاسيكية إلى جانب أدوات وتقنيات إلكترونية حديثة.

خلقت وضعية العتبة مواطنة هشة، تبرز هشاشتها عند تصادم الهوية الوطنية بهوية المواطنة التي تنعكس في سياسات السيطرة والملاحقة التي تمارسها الدولة، ولا سيما في الأحداث المفصلية الجماعية الجامعة، على سبيل المثال ما حدث في السنوات الأخيرة عند التصدي لمخطط برافر(2013) وهبة أيّار (2021) والحرب على غزة (2023).

عكفت الحكومة الإسرائيلية منذ بدايتها على استخلاص العبر في التعامل مع مواطنيها الفلسطينيين وابتكرت آليات للسيطرة والقمع بحسب الأحداث الجماعية التي تصدت لسياسات السيطرة والمحو. فعلى سبيل المثال بعد التصدي لمخطط برافر (2013) والذي استخدم منظموه الإنترنت ومنصات التواصل الاجتماعي، أسست النيابة العامة الإسرائيليّة في العام 2015 "الوحدة الإلكترونية" بغية مواجهة التحديات في البيئة الرقمية، ومحاربة الجريمة الإلكترونية والإرهاب الرقمي، بحسب تصريحهم. وقد تحوّلت هذه الوحدة إلى أداة رئيسية في مراقبة وملاحقة المحتوى الفلسطيني في الفضاء الرقمي الذي يشمل، علاوة على الملاحقة، محو المحتوى وحجب المواقع الإلكترونية.[2] وقد صرحت هذه الوحدة بأنها على تواصل دائم مع شركات مواقع التواصل الاجتماعي، فيسبوك ويوتيوب على سبيل المثال. ومنذ بداية ممارسة عملها، قدمت هذه الوحدة عشرات آلاف من طلبات إزالة وحذف للمحتوى الممنوع بموجب القوانين الإسرائيلية وبحسب معايير المجتمع لمواقع التواصل ذاتها. وتشير التقارير إلى أن هناك قفزة استثنائية في مدى

1. غانم، هنيدة مقتبس لدى: عنبتاوي، خالد. (2023). هبة في وضعية العتبة: دراسة في هبة الكرامة في الداخل الفلسطيني. **عُمران**، 46(12). ص 105-147.

2. AbuShanab, Anan. (2018). **Hashtag Palestine 2018: An overview of digital rights abuses of Palestinians**. 7amleh – Arab Center for Social Media Advancement..

تجاوب شركات مواقع التواصل الاجتماعي مع هذه الطلبات، فمثلًا في حين استجابت شركة فيسبوك (ميتا لاحقًا) لبضع مئات من الطلبات الإسرائيلية لإزالة المحتوى الفلسطيني عام 2015، وصل عدد الطلبات المقبولة عام 2019 إلى نحو 20,000.[3]

وفي العام 2021، وبعد محاولات إخلاء بيوت فلسطينية والاستيلاء عليها من قبل مستوطنين في حي الشيخ جرّاح في القدس، انطلقت مظاهرات وحملات دعم وتنديد فلسطينيّة في كافة المناطق -في الضفة الغربية وقطاع غزة والداخل-. تطورت المظاهرات في المدن والقرى العربية في الداخل لمواجهات غير مسبوقة، إذ شارك في الاعتداء على المواطنين الفلسطينيين في إسرائيل جماعات يمينية متطرفة ومستوطنون من الضفة الغربية وتمركزت هذه المواجهات في مدن الساحل. تميزت هذه الهبة - هبة أيّار -2021 باستخدامها المكثف لشبكة الإنترنت ومنصات التواصل الاجتماعي، أما الرد الإسرائيلي الرسمي على هذه الهبة كان قاسيًّا ومتنوعًا بأساليبه بغية كي وعي الشباب الذي شارك في المظاهرات والحملات. فإلى جانب الاعتداء الجسماني على المتظاهرين شنت الحكومة الإسرائيلية حملة اعتقالات ما زالت مستمرة حتى اليوم. استهدفت هذه الاعتقالات وتستهدف من شارك في المظاهرات ومن كتب منشورات دعم أو تنديد على مواقع التواصل الاجتماعي. رد الفعل الإسرائيلي هذا خلق حالة من الذعر والرعب في صفوف الفلسطينيّين المواطنين في إسرائيل. واليوم ونحن في خضم الحرب على غزة نرى إسقاطات هذه الحالة، فعلى الرغم من قسوة المشاهد التي تأتي من قطاع غزة، وعلى الرغم من مشاهد التضامن العالمي مع الشعب الفلسطيني ومع أهل القطاع إلا أن غالبية المواطنين الفلسطينيين في إسرائيل التزموا الصمت في الأشهر الأولى من الحرب، ومن لم يلتزم الصمت وعبر عن مشاعره لا سيما على منصات التواصل الاجتماعي وجد نفسه ملاحقًا ومعتقلًا ومتهمًا بالإرهاب، وهذا ما عزز من ممارسات القمع الذاتي وخلق حالة من عدم الثقة واللامبالاة لديهم.

على الرغم من تحوّل شبكة الإنترنت إلى فضاء لممارسة الحقوق السياسية والتعبير عن الذات وإعلان الهويات الوطنية، إلا أنها كشفت عن العديد من التحديات والتعقيدات والتناقضات. فعلى سبيل المثال، خرق مبدأ حياد شبكة الإنترنت الذي يحتّم على الحكومات والشركات بأن تعامل المستخدمين كافة وفق مبدأ المساواة وعدم التمييز، أو فرض الرقابة على المحتوى من جهات أمنية رسمية أو خاصة، مما قد يضع حرية الأفراد وأمنهم الرقمي عند استخدامها ومجمل الحقوق الرقمية على المحك.

وفي سياقنا المحلي، لا تكتفي دولة إسرائيل بعمل الوحدة الإلكترونية في تطوير وتوظيف تكنولوجيا الرقابة على الفلسطينيين، إنما تسعى حثيثًا إلى تشريع سياستها من خلال سَنّ القوانين التي توسع صلاحياتها في ملاحقة الفلسطينيين والمحتوى المتضامن مع القضية الفلسطينية. ففي عام 2016، صادق الكنيست على "قانون مكافحة الإرهاب الذي يحاول ببنود فيه تجريم العمل السياسي وتقويضه وتعريفه كإرهابي" الذي يهدف إلى قمع نضال فلسطينيي الداخل، وهذا يُعدّ انتهاكًا خطيرًا لحرية التعبير، فقد سمح القانون لأجهزة دولة إسرائيل ملاحقة فلسطينيي الداخل على خلفية نشاطات تعبر عن تضامنهم مع الفلسطينيين في الضفة الغربية وقطاع غزة. وفي السياق ذاته، صادقت اللجنة الوزارية للتشريعات التابعة للحكومة الإسرائيلية على مشروع "قانون فيسبوك المجدَّد"، الذي جاء امتدادًا لمقترحات تشريعية سابقة بادر إليها عام 2016 وزير الأمن الداخلي آنذاك جلعاد إردان، وعام 2017 وزيرة القضاء آنذاك أييليت شاكيد.

3. Luke Goldstein, Luke. (2021, July 12). How a secretive cyber unit censors Palestinians," **The American Prospect**.

يستهدف مشروع القانون هذا، المحتوى الفلسطيني على شبكات التواصل الاجتماعي ويسعى لشطب المحتوى المتضامن مع القضية الفلسطينية. وبحسب نص مشروع القانون، فإن شركة فيسبوك عليها أن تمنح النيابة الإسرائيلية صلاحيات واسعة لحذف المحتوى المنشور على شبكات التواصل الاجتماعي والمواقع الإلكترونية بتهمة "التحريض"، ويتيح مشروع القانون لأجهزة الأمن الإسرائيلية ملاحقة أصحاب هذا المحتوى قضائيًّا وتوجيه تهمة ارتكاب مخالفة جنائية. والأخطر من ذلك، أن مشروع القانون هذا يمنح الصلاحية للمدعي العام الإسرائيلي باستخدام "أدلة سرية" تتيح إزالة المحتوى وتحرم أصحاب هذا المحتوى من فرصة الدفاع عن أنفسهم. يمكن اعتبار هذا القانون نقطة تحوّل في طبيعة العلاقة بين السلطات الإسرائيلية وشركات التواصل الاجتماعي، إذ أصبحت علاقة الامتثال الطوعي إلتزامًا بمحاربة المحتوى تحت طائلة القانون. يذكر أن معظم قضايا التجريم على خلفية حرية التعبير عن الرأي في الفضاء الرقمي، تستند إلى قانون مكافحة الإرهاب والقانون الجنائي.

باتت الملاحقة السياسية والأمنية بتهم التحريض على شبكات التواصل الاجتماعي هاجسًا للشباب الفلسطينيين، ففي استطلاع نشره المركز العربي لتطوير الإعلام الاجتماعي- حملة عام 2019، عبر 59% من الشباب الفلسطيني في الضفة الغربية وقطاع غزة والداخل أنّ من أكثر معوّقات استخدام الإنترنت ومواقع التواصل الاجتماعي هي الرقابة المفرطة فيها، و 33.6% من الشباب أكدوا أنهم تعرضوا للمساءلة نتيجة تعبيرهم عن آرائهم السياسية في شبكات التواصل الاجتماعي والمواقع الأخرى. إن الإحساس العميق بوجود رقابة أمنية على المنشورات والمحتوى، إلى جانب الملاحقة الفعلية للنشطاء والصحفيين والأفراد الناشطين على شبكات التواصل الاجتماعي، خلق حالة من الرقابة الذاتية العالية لدى قطاع واسع من المجتمع الفلسطيني لا سيما في الداخل، مما أدى إلى حالة من الردع الذاتي والنأي عن ممارسة حقهم في حرية التعبير والمشاركة السياسية.

تداعيات ما بعد 7 أكتوبر: حرب على الوجود الفلسطيني

في 7 أيّار 2023، قُدّم للكنيست اقتراح تعديل جديد على قانون "مكافحة الإرهاب"، بحيث يتيح التعديل المقترح للأجهزة الأمنية الإسرائيلية ملاحقة من تصفهم بداعمي الإرهاب، وتخوّل دولة إسرائيل الأجهزة الأمنية تعريف ما هو "الإرهاب". وقد صادق الكنيست بتاريخ 8 تشرين الثاني (2023) على التعديل التاسع، والمتعلق باستهلاك "المنشورات الإرهابية"، حيث ينص القانون الجديد على عقوبة السجن لمدة عام لكل من يطلع بانتظام ومنهجية على محتوى يعتبره القانون الإسرائيلي أنه "محرض على الإرهاب". وقد أدخل هذا التعديل تطورًا جديدًا في الصلاحيات الممنوحة لأجهزة الأمن الإسرائيلية بحيث أصبح يتيح ملاحقة الفلسطينيين على أساس متابعتهم أو تفاعلهم أو مشاركتهم لمحتوى تعتبره إسرائيل محرضًا، دون شرط القيام بأعمال ونشاطات. وعلى أساس هذا القرار، يمكن لأجهزة الأمن الإسرائيلية محاكمة الفلسطينيين على أساس "النية"، وهو انتهاك بالغ الخطورة للحق في حرية التعبير والخصوصية.[4]

4. حملة. (2024). **هاشتاغ فلسطين 2023: الحقوق الرقمية الفلسطينية في الحرب**. حملة - المركز العربي لتطوير الإعلام الاجتماعي.

يهدد هذا القرار ويستهدف فلسطينيي الداخل مباشرة، ويفرض طوقًا خانقًا عليهم لردعهم عن التضامن مع شعبهم ضد الإبادة الجماعية في قطاع غزة. ولابد من الإشارة، إلى أنه ومنذ أحداث 7 أكتوبر 2023، تصاعد استهداف فلسطينيي الداخل من قبل الحكومة الإسرائيلية، بواسطة ممارسات شملت الملاحقة والاعتقال والفصل التعسفي من العمل والإقصاء من الجامعات على خلفية إبداء التضامن مع الفلسطينيين في قطاع غزة. إن هذا الاستهداف ما هو إلا عدوان هستيري على الوجود الفلسطيني وهندسة وكيّ للوعي في كل ما يتعلق بحقوقه وقضاياه وتاريخه.[5]

وفي ورقة موقف بشأن قانون "استهلاك المنشورات الإرهابية" الإسرائيلي أصدرها المركز العربي لتطوير الإعلام الاجتماعي – حملة، ورد فيها "أن هذا القانون يمس بشكل سافر بفلسطينيي الداخل والقدس، وهو قانون من شأنه أن يؤدي إلى زيادة في مستوى الرقابة والتعدي على حقوقهم في الخصوصية والتعبير والمعرفة. وثمة تخوّف حقيقي من أن يجعل هذا القانون مسألة الاطلاع على الوثائق الإخبارية جريمة جنائية، بحيث يمكن أن يتحوّل مجرد الاطلاع على معلومات إخبارية إلى تهمة "التماهي والتعاطف مع الإرهاب".[6]

وفي مؤتمر الانترنت و الديجيتال الذي عُقد في شهر يونيو/حزيران 2024 عرضت الباحثة هامة أبو كشك نتائج استطلاع رأي يتناول نشاط الفلسطينيين في إسرائيل في ظل الحرب على غزة والملاحقات، من هذه النتائج 56% من المشتركين قالوا إنهم سمعوا عن قانون "محاربة الإرهاب"، و 70% من الذين سمعوا عن القانون صرحوا أن نشاطهم الإلكتروني انخفض بسبب هذا القانون. وخلصت نتائج البحث الذي عرض في المؤتمر إلى أن هذه القوانين تؤدي إلى إخراس المجتمع العربي على منصات التواصل الاجتماعي، بالمقابل تتجاهل التحريض والملاحقات التي تأتي من أطراف إسرائيلية يهودية؛ أي أن القانون يستهدف مباشرة المواطن الفلسطيني بإسرائيل.[7] وفي الفترة ما بين 7 أكتوبر/ تشرين الأول و14 نوفمبر/ تشرين الثاني، أرسلت السلطات الإسرائيلية إلى شركات التواصل الاجتماعي ما مجموعه 9,500 طلب إزالة/حذف منشورات، وما يعادل 60% منها أُرسِل إلى ميتا مع معدل امتثال يبلغ 94%[8].

تهدف هذه الدراسة إلى بحث مفهوم الأمان الرقمي لدى الشباب الفلسطيني في الداخل، من خلال توفير بيانات حديثة حول طبيعة وخصائص استخدام الشباب الفلسطينيين لشبكة الإنترنت. وتهدف إلى التعرف على التحديات والتهديدات للشباب الفلسطينيين والمؤسسات ذات الصلة والفرص الأساسية المتاحة أمامهم، فيما يتعلق بحماية حقوقهم الرقمية وتمكينهم بكل ما يخص الأمان الرقمي، أملا بالإسهام في تعزيز حماية الحقوق الرقمية، والانخراط في المناصرة الاستراتيجية، ومعالجة الانتهاكات في مجال السلامة والأمان الرقمي.

5. وتد، محمد. (2023). **كيف يهدد تعديل قانون "محاربة الإرهاب" فلسطينيي 48؟**. الجزيرة نت.

6. حملة. (2023، 20 تشرين الثاني). **ورقة موقف بشأن قانون حظر استهلاك المنشورات الإرهابية الإسرائيلي**. **حملة**- المركز العربي لتطوير الإعلام الاجتماعي.

7. أبو كشك، هامة. (2024، 10 حزيران). **لولب الإخراس: المساحة الرقمية في المجتمع العربي** (محاضرة). وِبّنا: مؤتمر الانترنت والديجيتال في المجتمع العربي. أم الفحم: مركز الخوارزمي.

8. Brewster, Thomas. (2023, Nov 14). Israel has asked Meta and TikTok to remove 8,000 posts related to Hamas War. **Forbes**.

أسئلة البحث:

تحاول الدراسة أن تجيب عن الأسئلة الرئيسية التالية:

ما طبيعة معرفة الشباب الفلسطيني في الداخل بمفاهيم الأمان الرقمي وما مدى وعيهم بالمخاطر الرقمية التي يمكن أن تواجههم؟ وما مدى تعرضهم لهجمات واعتداءات رقمية؟ وما هو واقع المساءلة والتحقيق من جهات أمنية إسرائيلية أو جهات اجتماعية على خلفية نشاطهم الرقمي؟ وما أثر سياسات المنصات على نشاطهم منذ بدء الحرب على قطاع غزة؟ وما طبيعة التهديدات والتحديات والمخاطر التي تواجه الناشطات والمدافعات عن حقوق الإنسان في الداخل؟

الباب الثاني

منهجية الدراسة

أدوات البحث:

تسعى هذه الدراسة إلى الكشف عن حالة الأمان الرقمي في تجربة استخدام الشباب الفلسطيني والمدافعات عن حقوق الإنسان لشبكة الإنترنت، وذلك بهدف اعتماد النتائج لتكون منطلقا للعمل من أجل تعزيز حماية الحقوق الرقمية للشباب الفلسطيني في الداخل، وقد استخدم الباحث لهذا الغرض آليات البحث الكمي والكيفي من أجل استخلاص نتائج واستنتاجات علمية تحقق أهداف البحث.

وارتكز البحث على إطار نظري تضمن مراجعة للأدبيات العلمية، واستخدم، بهدف جمع البيانات الخاصة بالبحث، أداتين بحثيتين لقياس وإدراك واقع المخاطر الرقمية في الداخل، الأولى: عبارة عن استطلاع/ مسح ميداني، (شارك فيه 409 مستطلَعين(، أما الأداة الثانية فكانت عبارة عن لقاءات مع مجموعات تركيز (مجموعات بؤرية).

المسح الميداني:

استخدم المسح الميداني استمارة بحثية تكونت من 27 سؤالًا موزعة على خمسة محاور وهي:

أوّلًا، خصائص المستطلعين وبياناتهم الشخصية، مكان سكناهم والنوع الاجتماعي، والتحصيل العلمي.

ثانيًا، طبيعة وخصائص استخدام شبكة الإنترنت: من حيث مكان الاتصال بالإنترنت وعدد ساعات الاستخدام، وطبيعة الحسابات على المنصات.

ثالثًا، مقدار الوعي والمعرفة بالأمان الرقمي والوعي بالمخاطر الرقمية وطبيعة التهديدات التي تعرض لها المستطلَعين، وكيف كان تصرفهم حيالها.

رابعًا، مدى تعرض المبحوثين للمساءلة والتحقيق من قبل جهات أمنية أو اجتماعية على خلفية ما يُنشر على المنصات.

خامسًا، أثر سياسات المنصات على نشاط الشباب الفلسطيني منذ بدء الحرب على قطاع غزة.

مجموعات التركيز:

لقد استخدمت الدراسة مجموعات التركيز (البؤرية) كأداة ثانية من أجل تعميق نتائج الدراسة الكمية، ولأجل هذا الغرض عقدت أربعة لقاءات مع المجموعات البؤرية وذلك على مدار شهري شباط وآذار 2024. ونُظمت كل اللقاءات عبر تطبيق زووم، يسّرتها الباحثة أفنان كناعنة.

جدول (1): توزيع المجموعات البؤرية بحسب الفئة والمنطقة الجغرافية والجنس وعدد المشاركين وطريقة عقد اللقاء

	تعريف المجموعة	المنطقة	عدد المشاركين	النوع الاجتماعي		طبيعة إجراء اللقاء
				إناث	ذكور	
1	طلبة المراحل الثانوية	مدينة الناصرة ومحيطها	5	5 إناث	-	زووم
2	الشباب وطلبة الجامعات	النقب	6	5 إناث	1 ذكور	زووم
3	طلبة الجامعات	الداخل عدا النقب	6	4 إناث	2 ذكور	زووم
4	مجموعة المدافعات عن حقوق الإنسان	الداخل	6	6 إناث	-	زووم
	المجموع	-	**23**	**20**	**3**	-

وتضمنت محاور النقاش في مجموعة طلبة المراحل الثانوية: استخدام الطلبة لشبكة الإنترنت، وطبيعة المنصات التي يستخدمونها ويتواجدون عليها، وأهدافهم من استخدام الإنترنت، وطبيعة التهديدات الرقمية التي يتعرضون لها، ومدى شعورهم بالأمان أثناء تواجدهم على المنصات الرقمية، ومدى توفر إجراءات الأمان في بيت العائلة، وطبيعة استخدام الإنترنت في ظرف العدوان على قطاع غزة. والتدريبات التي تلقوها حول الحقوق الرقمية والأمان الرقمي، ونظرتهم لمستقبل استخدام الشبكة.

أما محاور النقاش الخاصة بطلبة الجامعات فتكونت من: طبيعة العلاقة بشبكة الإنترنت ومراحل تطورها، والتجارب التي مروا بها في علاقتهم مع الشبكة، والمنصات التي يستخدمونها ودوافعهم وراء ذلك الاستخدام، وطبيعة التهديدات التي تعرضوا لها، وفيما إذا كانوا قد تعرضوا لتدريبات ترفع من وعيهم في الأمان الرقمي، ورؤيتهم للحلول المرتبطة بتراجع حالة الأمان الرقمي، وكذلك رؤيتهم للمستقبل.

أما محاور النقاش الخاصة بالمدافعات عن حقوق الإنسان فتكونت من ثلاثة محاور رئيسية، أوّلها، طبيعة التجربة المرتبطة باستخدام المشاركين للبيئة الرقمية وأنواع التهديدات الرقمية التي تعرضن لها، والجهات التي تقف خلفها؛ ثانيًا، مدى وعي المؤسسات التي يعملن بها بالهجمات الرقمية؛ ثالثًا، أثر الحرب على غزة على نشاطهن الرقمي.

عُقدت الحوارات والنقاشات باللغة العربية بين المحكية والفصحى، واختلفت بنيتها ومكونات الأسئلة فيها تبعا للفئة التي تمثلها المجموعة، وكذلك تبعًا لموقفها وطبيعة عملها وعلاقتها مع موضوع البحث.

الباب الثالث

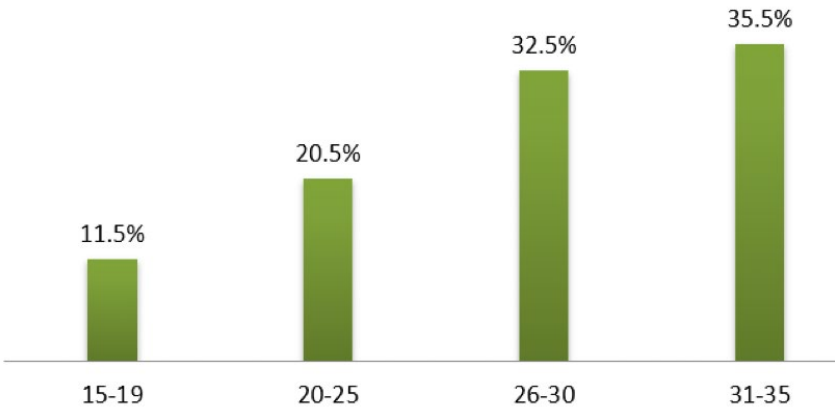
نتائج الدراسة التحليلية

أوّلا: نتائج الاستطلاع والمجموعات البؤرية

كانت أداة البحث الأولى عبارة عن استطلاع رأي هاتفي، نفذته شركة "داتا نيو فيجن" المتخصصة بالأبحاث والدراسات المسحية. وشملت عينة المسح (409) مجيبا من المدن والبلدات العربية في الداخل.

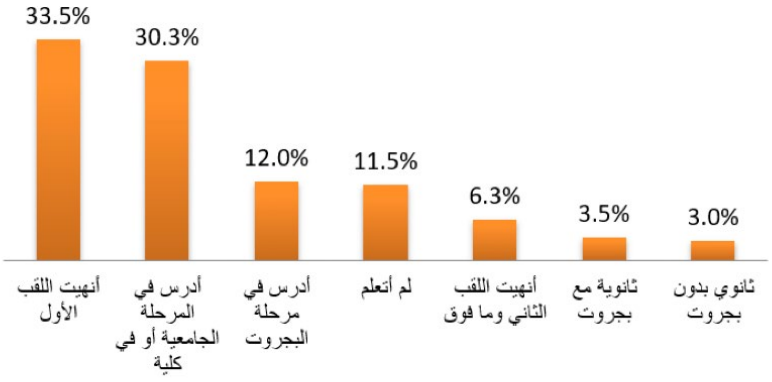
المحور الأوّل: خصائص المبحوثين

1. توزيع المستطلَعين بحسب الفئة العمرية:



شكل رقم(1) الفئة العمرية للمستطلعين

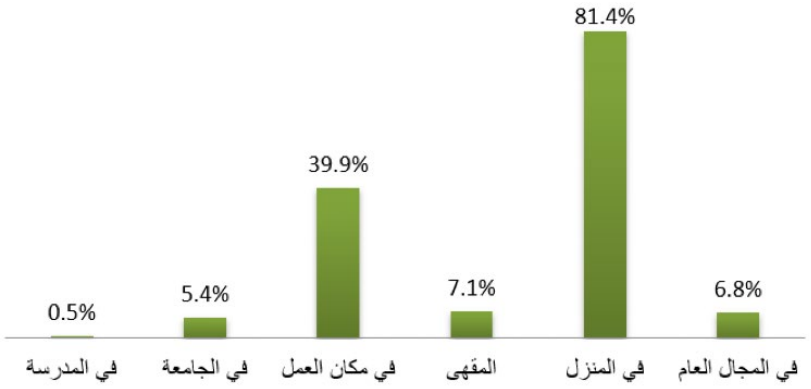
2. مستوى التحصيل العلمي للمستطلَعين:



شكل رقم (2) يظهر مستوى التحصيل العلمي للمستطلعين

المحور الثاني: خصائص استخدام الشباب لشبكة الإنترنت:

1. مكان الاتصال بالإنترنت:

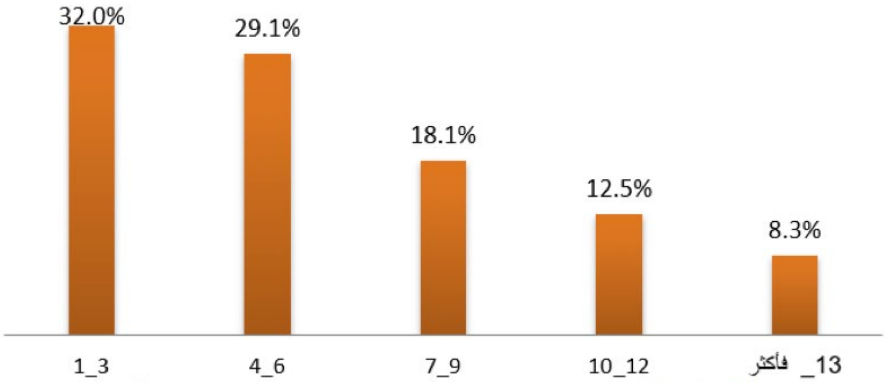


شكل رقم (3) توزيع إجابات المستطلعين على غالبية اتصالهم بالإنترنت

ردا على هذا السؤال كان بإمكان المستطلَعين الإجابة بأكثر من اختيار. تُظهر النتائج أن غالبية المستطلَعين يستخدمون الإنترنت في المنزل وذلك بنسبة 81.4%، تلاها في "مكان العمل" بنسبة 39.9%. وبنسب متقاربة يستخدمون الإنترنت في المقاهي (7.1%) والمجال العام (6.8%) والجامعة (6.8%).

وتشير النتائج السابقة (شكل 3) إلى تراجع نسبة استخدام شبكة الإنترنت في المقهى والجامعة والمجال العام، مقابل ارتفاع نسبة الاستخدام في المنزل، نعزو هذا الانخفاض إلى وجود مخاوف وعدم إحساس بالأمان الرقمي في استخدام الشبكات التي توفرها المقاهي والجامعات وتتوفر في الأماكن العامة من ناحية، وإلى وجود خدمات اتصال حديثة من خلال خدمة الإنترنت التي تطرحها شركات الاتصال الإسرائيلية عبر شريحة الجوال (3G و4G وG5) من ناحية ثانية. ورغم احتمالية صواب هذا التحليل المرتبط بجودة خدمات الإنترنت إلا أن النقاش مع المشاركين في المجموعة البؤرية التي نظمت مع الشباب في منطقة النقب جنوبا أشاروا إلى ضعف خدمات الإنترنت في تلك المناطق المهمشة وغير المعترف بها سياسيا وتنظيميا، وهي مسألة انعكست على مسار النقاش الذي عقد افتراضيا عبر تطبيق زووم، لقد واجهت ميسرة اللقاء مشاكل في الشبكة أعاقت حديث بعض المشاركين/أت فيما انسحب بعضهم بسبب سوء الخدمة وعدم القدرة على الحديث.

2. عدد ساعات استخدام الإنترنت:

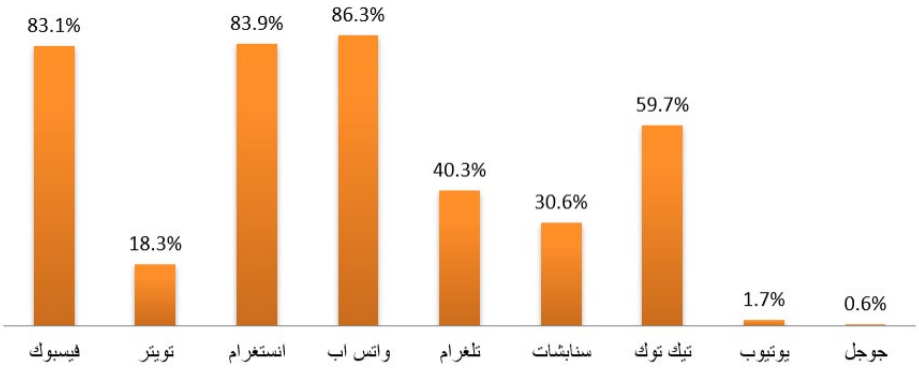


شكل رقم (4) يظهر نسبة عدد ساعات استخدام المستطلعين للإنترنت يوميًّا

يظهر الشكل (4) عدد ساعات استخدام الإنترنت يوميًّا بالنسبة للمبحوثين، وتشير النتائج أن نحو 32% من الشباب يستخدمون الإنترنت ما بين 1-3 ساعات يوميًّا، ونسبة 29.1% يستخدمون الإنترنت ما بين 4-6 ساعات يوميا، ونسبة 18.1% يستخدمون الإنترنت نحو 7-9 ساعات يوميا، ونحو 12.5% يستخدمون الإنترنت ما بين 10-12 ساعة يوميا، و8.3% يستخدمون الشبكة أكثر من 13 ساعة يوميا.

وتعكس النتائج نسبًا مرتفعة من التواجد على الشبكة، إذ يستخدم ما يقارب نصف المستطلَعين الشبكة ما بين 4-9 ساعات يوميا. وقد عكست النقاشات مع المجموعات المركزة وتحديدا الشباب وطلبة المراحل الثانوية أن أساس تواجدهم على الشبكة هو لمتابعة الأخبار، وأشاروا أن تفاعلهم ونشاطهم الرقمي تراجع. وأظهرت المناقشات مع الشباب أنهم يحرصون على إلغاء خاصية النشر العام واقتصار جمهورهم على الأصدقاء والدوائر الاجتماعية المغلقة.

3. أنواع الحسابات على مواقع التواصل الاجتماعي:



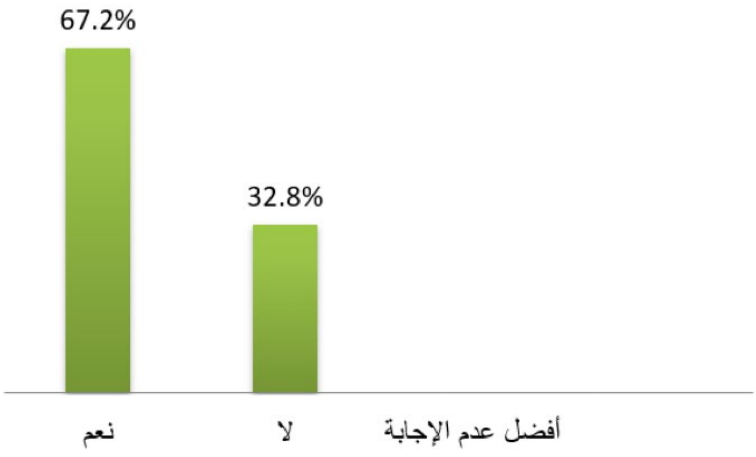
شكل رقم (5) نسب استخدام المستطلعين لمواقع التواصل الاجتماعي أو امتلاك حساب فيها

في الإجابة عن هذا السؤال استطاع المستطلَعين اختيار أكثر من إجابة. يُظهر الشكل (5) توزيع نشاط المستخدمين (استخدام أو امتلاك حساب) على مختلف منصات التواصل الاجتماعي. وجدنا أن 86.3% منهم يستخدمون تطبيق المراسلة والتواصل "واتس أب"، تلاه تطبيق الانستغرام وذلك بنسبة 83.9%، منصة فيسبوك بنسبة 83.1%، وتطبيق تيك توك بنسبة 59.7%، ويستخدم تلغرام 40.3% منهم، وسناب شات يستخدمه 30.6%، وأخيرا شبكة "إكس" (تويتر سابقا) يستخدمها 18.3% من المستطلَعين.

وتعكس النتائج أعلاه أن مجموعة من التطبيقات والشبكات الاجتماعية مثل: "واتس اب" و"انستغرام" و"فيسبوك" و"تيك توك" و"تلغرام" تحتل الصدارة بين المستخدمين. تدل النتائج إلى كثافة استخدام المستطلَعين لأكثر من تطبيق مراسلة أو شبكة تواصل، وقد تكون الأسباب لهذا تزايد غايات التراسل الفوري ومتابعة الأخبار الآنية في ظل الأحداث السياسية الساخنة. وهو ما عكسه النقاش في المجموعات البؤرية حيث لجأ جانب من المشاركين إلى العودة للمنصات من أجل متابعة الأحداث والأخبار اليومية في ظل عدم قدرتهم من التعبير عن أنفسهم في الفضاءات العامة في الدولة.

المحور الثالث: معرفة الأمان الرقمي وإدراك المخاطر الرقمية

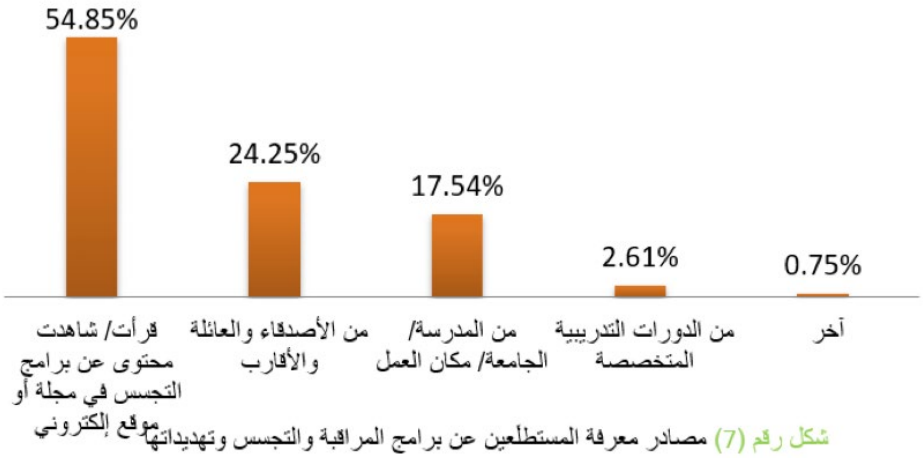
1. معرفة المستطلَعين ببرامج التجسس وتهديداتها:



شكل رقم (6) مدى معرفة المستطلعين ببرامج التجسس وتهديداتها

طرح الاستطلاع على المستطلَعين سؤالًا حول مدى معرفتهم ببرامج التجسس وتهديداتها، تُظهر النتائج أن نسبة 67.2%، من المستطلعين سمعوا عن برامج التجسس وتهديداتها، في حين ظهر أن 32.8% منهم لم يسمعوا بهذه البرامج مطلقًا. وتُعتبر نسبة مَن لم يسمع عن برامج التجسس عالية نسبيًّا في ظل تزايد الهجمات الرقميّة، ولا سيما تلك المتعلقة ببرامج التجسس وتحديدًا المطوَّرة في إسرائيل. نرى هذه الأرقام في عين القلق على الرغم من أن ثلثي المستطلعين يعرفون أو على الأقل سمعوا بهذه البرامج، ولكن يظل السؤال ما هي مصادر معرفتهم، وهو ما سنجيب عنه في الشكل التالي.

2. مصادر المعرفة عن برامج المراقبة والتجسس وتهديداتها

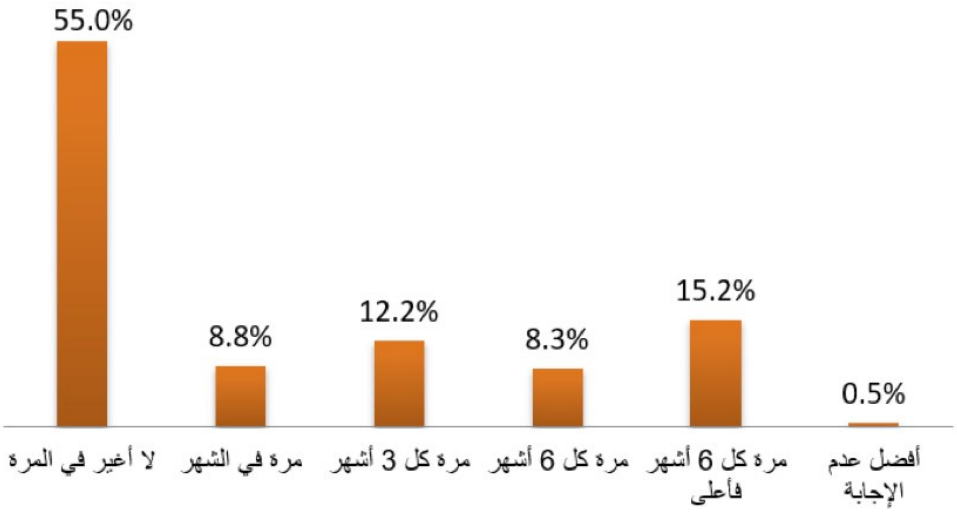


شكل رقم (7) مصادر معرفة المستطلعين عن برامج المراقبة والتجسس وتهديداتها

يظهر الشكل (7) إجابات المستطلعين عن مصادر معرفتهم ببرامج المراقبة والتجسس وتهديداتها. تبين أن أكثر من نصف المستطلَعين (54.8%) سمعوا أو تعرفوا على هذه البرمجيات من خلال القراءة أو المشاهدة حول هذه البرامج من "مجلة أو موقع الكتروني"، و 24.2% من المستطلَعين سمعوا عن ذلك من "الأصدقاء والعائلة والأقارب"، و 17.5% سمعوا عنها من "المدرسة أو الجامعة أو مكان العمل"، ونحو 2.6% فقط سمعوا عنها من خلال "الدورات التدريبية المتخصصة".

وتعكس النتائج السابقة ارتفاعا في نسبة المعرفة التي تعتمد على القراءة أو مشاهدة المواقع الإلكترونية، وقابل ذلك تراجع المعرفة المتخصصة والتي مصدرها الدورات التدريبية، وهو ما يؤكد على صحة الاستنتاج الذي تحدثنا عنه في السؤال السابق، فبرامج التجسس وطبيعة تهديداتها تحتاج إلى معرفة متخصصة وعميقة في ظل طبيعة التهديدات وحجمها والجهات التي تقف خلفها.

3. وتيرة تغيير كلمة السر (كلمات المرور في الحسابات المختلفة)

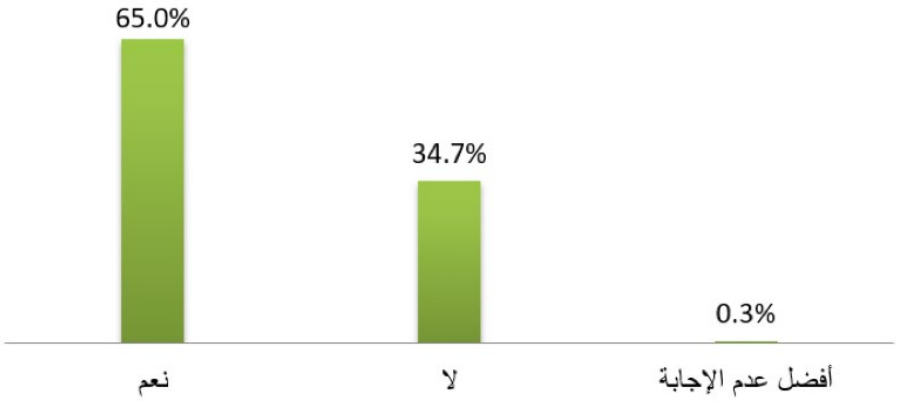


شكل رقم (8) توزيع إجابات المستطلعين لوتيرة تغيير كلمة المرور

بهدف معرفة مدى قيام المستطلَعين بمجموعة من المهام والإجراءات التي تعتبر من أساسيات الأمان الرقمي، طُرحت عليهم مجموعة من الأسئلة التي كان من ضمنها: "ما هي وتيرة تغيير كلمة المرور على حساباتكم"، حيث تبين أن نحو 55% من المستطلَعين لا يغيرون كلمات المرور بالمرة، في حين تبين أن 15.2% من الشباب يغيرون كلمات المرور مرة كل 6 أشهر فأعلى، وأن نحو 2.12% يغيرون كلمات المرور مرة كل 3 أشهر، و8.8% من المبحوثين يغيرون كلمات المرور مرة كل 6 أشهر، ونحو 8.8 % يغيرون الكلمات مرة في الشهر.

وتدل النتائج إلى غياب الوعي بالمعرفة المرتبطة بأهمية تغيير كلمات المرور، وهي مسألة تعتبر من أساسيات الممارسات لضمان أبسط أشكال تأمين الوجود الرقمي، وهذا مؤشر لغياب الوعي بمصادر التهديد لدى أكثر من نصف المستطلَعين. ومن الجدير ذكره أن معرفة أهمية تغيير كلمات المرور لا يترجم بالضرورة لممارسات وقائية.

4. إعدادات الأمان على الشبكات الاجتماعية

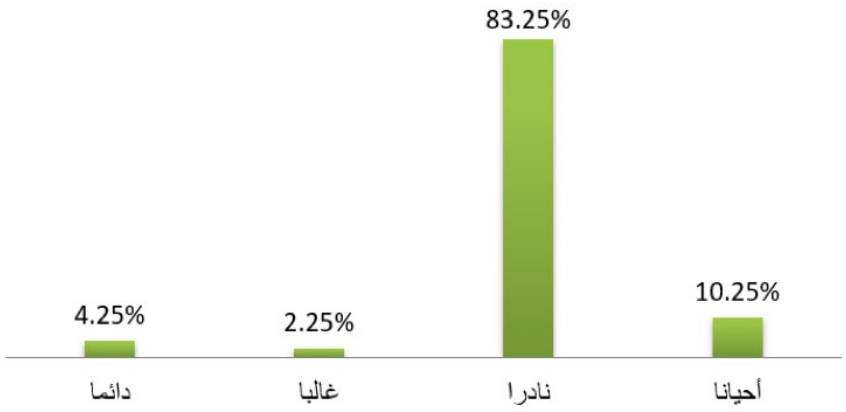


شكل رقم (9) نسبة المشاركين الذين يحددون إعدادات الأمان

أظهر الاستطلاع أن نحو 65% من المستطلَعين يحددون إعدادات الأمان على شبكات التواصل، بينما بلغت نسبة من لا يقومون بذلك 34.7%.

وتعتبر إعدادات الأمان والخصوصية على الشبكات الاجتماعية مسألة غاية في الأهمية بالنسبة لصفحات الأفراد أو المجموعات والمنظمات، وهي تتضمن مجموعة من الأسئلة الرئيسية على المستخدم أن يطرحها على نفسه أثناء تحديد هذه الإعدادات، تتيح الاجابة عنها قائمة من الخيارات التي تضمن للمستخدمين "مستوىً من الأمان" فيما لو استخدمت عن إدراك وعلى نطاق جيد. تعكس النتائج عدم قيام نحو ثلث المستطلَعين بتحديد إعدادات الأمان في حساباتهم على الشبكات الاجتماعية، وهو أمر تعزَّز تفسيره في النقاشات مع مجموعات التركيز حيث اضطر جانب كبير من المشاركين إلى إعادة ضبط الإعدادات وتحديدا الغاء خيار النشر العام في ظل تنامي المخاوف من مراقبة المحتوى وتصيّد النشطاء.

5. إضافة أشخاص غير معروفين على حساباتي على الشبكة

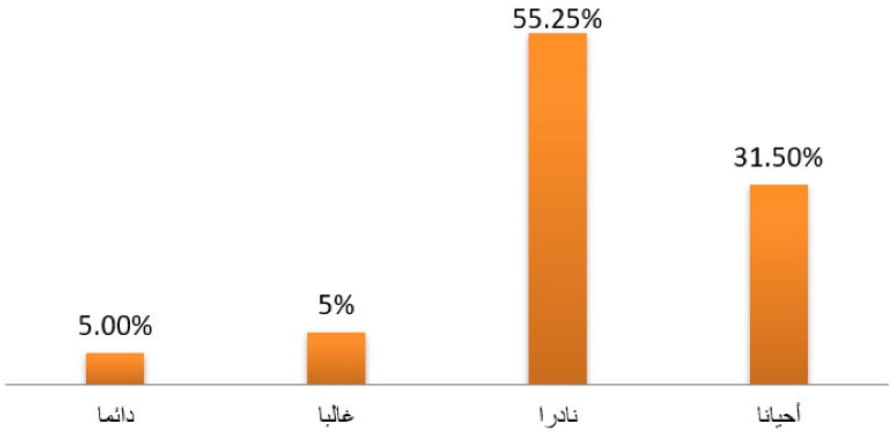


شكل رقم (10) وتيرة المصادقة على طلبات صداقة من أشخاص غير معروفين على الشبكة

طُرح على المستطلعة آرائهم سؤال: "أقوم بإضافة أشخاص لا أعرفهم بشكل شخصي على حساباتي على الشبكة" وظهر أن نحو 83.2% نادرًا ما يفعلون ذلك، فيما أجاب 10.2% بإنهم يفعلون ذلك "أحيانا"، و4.2% يفعلون ذلك "دائما"، و2.2% يفعلون ذلك غالبًا.

تحمل الإجابات السابقة مؤشرًا إيجابيًا إذ أن أكثر من ثلثي المستطلَعين الشباب لا يصادقون على طلبات صداقة من أشخاص لا يعرفونهم. وبيّنت النقاشات في المجموعات البؤرية أن المشاركات والمشاركين ذهبوا إلى أبعد من ذلك، فبعد الحرب على غزة بادروا إلى حذف أشخاص كانوا قد صادقوا على طلبات صداقتهم قبل الحرب، ولا سيما أشخاص فلسطينيين لا يعرفونهم جيدًا، أو ممن يخدمون أو خدموا في الجيش الإسرائيلي وأجهزة الدولة. هذا السلوك يمكن اعتباره مؤشرًا لأزمة الثقة التي تعمقت بعد الحرب، فالكثير ممن ظنوا أنهم أصدقاء أو أصدقاء لأصدقاءهم أصبحوا مصدر تهديد بعد بدء الحرب على قطاع غزة، حيث تضاعفت الضغوط والقمع والمساءلة الأمنية على منشورات سياسية أو تضامنية، وتضاعفت ممارسات الاستهداف والإساءة من خلال إعادة نشر منشورات على شبكات اجتماعية وجعلها مادة للإساءة والتشهير، وأحيانا للتحريض والتهديد بالقتل، وهو ما جعل المشاركين يحذفون مئات "الأصدقاء المفترضين" من صفحاتهم.

6. مشاركة صور أو أمور شخصية على الشبكة

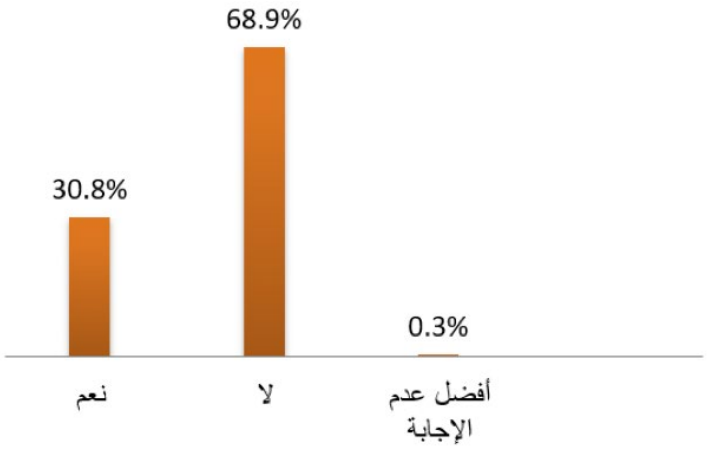


شكل رقم (11) وتيرة مشاركة الصور والأمور الشخصية على الشبكة

تُبيّن النتائج في الشكل (11) أن نحو نصف المستطلَعين لا يشاركون الصور والأمور الشخصية إلا في حالات نادرة (55.2%) وأحيانًا (31.5%)، بينما نسبة ضئيلة منهم يشاركون أمورهم الشخصية والصور بوتيرة عالية - غالبًا بنسبة 8.2%، ودائمًا بنسبة 5%.

يمكن الاستنتاج من هذه النتيجة أن ثمة اعتقاد سائد د بين المستخدمين أن الشبكة ليست آمنة، وأن هنالك مخاطر قد تترتب على مشاركة صور وأمور شخصيّة. ولا يمكننا الجزم أنّ من أجاب بنُدرة مشاركته الصور والأمور الشخصية فعل ذلك نتيجة معرفته بالمخاطر، فقد يكون ذلك نتيجة أسباب وعادات ثقافية. ومن الأهمية الإشارة إلى المخاطر النابعة من السياق الفلسطيني عند مشاركة الصور والأمور الشخصية، فهي قد تستخدم كمصدر لاستقاء المعلومات والرقابة.

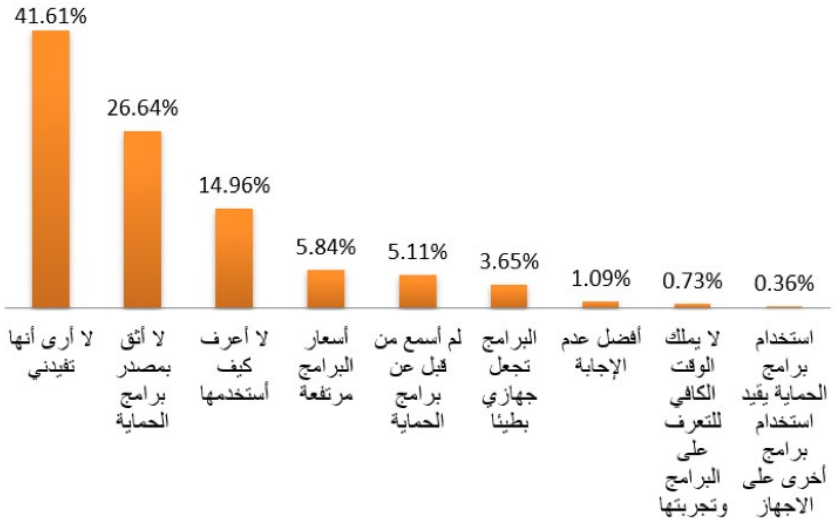
7. استخدام برامج الحماية على الشبكة:



شكل رقم (12) نسبة استخدام المستطلعين لبرامج الحماية

تشير النتائج إلى أن نحو 68.9% من المستطلَعين لا يستخدمون برامج حماية لأجهزتهم، بينما يستخدمها نحو ثلث المستطلَعين. سلوك المستخدمين هذا يعزز من فرص استهدافهم في البيئات الرقمية لا سيما فئة الشباب. ولعل السؤال الأبرز الذي علينا طرحه هنا: ما هي الأسباب التي تمنع ومنعت المستطلَعين من استخدام برامج الحماية الأساسية؟ سنجيب عن هذا السؤال في البند التالي.

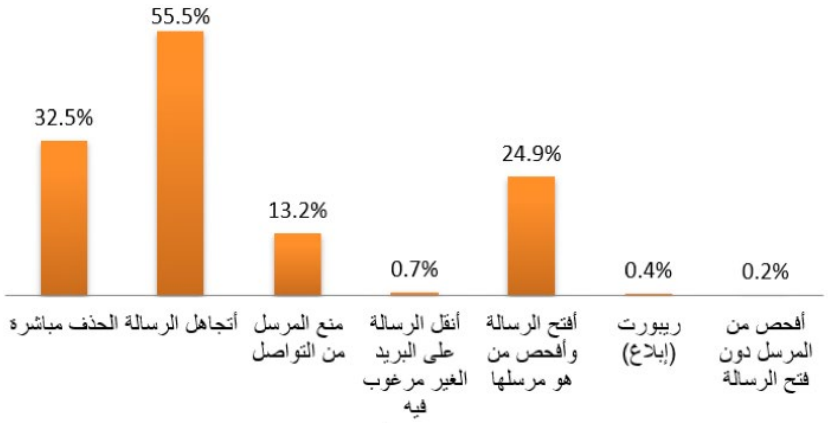
8. أسباب عدم استخدام برامج الحماية على الشبكة



شكل رقم (13) توزيع أسباب عدم استخدام برامج الحماية من قبل المستطلعين

تفسر نتائج هذا البند ما جاء في البند السابق من انعدام استخدام برامج الحماية. وقد برز سببان أساسيّان لعدم استخدام البرامج، أوّلهما أن المستخدمين لا يرون أي فائدة من برامج الحماية (41.6%)، وثانيهما أن المستخدمين لا يثقون بمصادر برامج الحماية (26.6%). تسلط هذه الأرقام الضوء على أزمة الثقة ومستويات الشك التي يعيشها الفلسطيني المواطن في إسرائيل. إلى جانب ذلك نحو (20%) من المستطلعين أسباب عدم استخدامهم لبرامج الحماية مصدرها معرفيّ، (14.9 %) منهم صرحوا أنهم لا يعرفون كيف يستخدمونها، و (5 %) قالوا أنهم لم يسمعوا بها من قبل. تعكس هذه النتائج فجوة عميقة في المعرفة وفرصة سانحة لنشر الوعي حول هذه البرامج والتدريب على استخدامها لا سيما في ظل الرقابة والقمع الذي يحيط بالمستخدمين.

9. السلوك عند استلام رسائل من مصدر مجهول

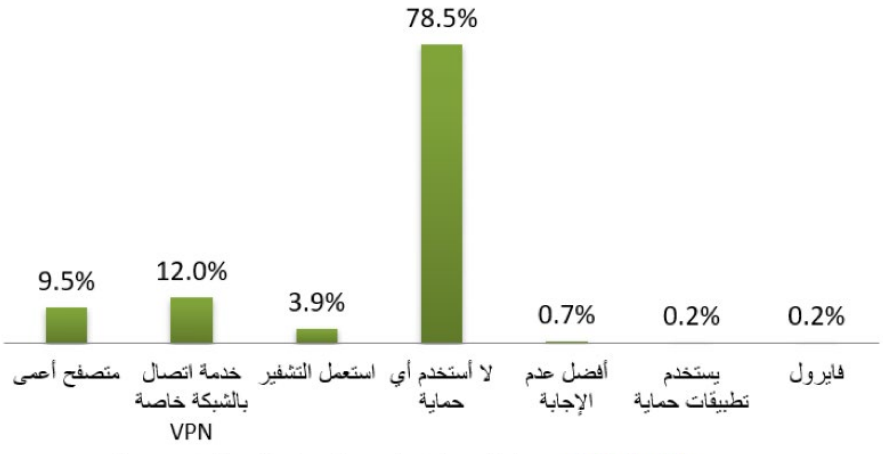


شكل رقم (14) توزيع سلوكيات المستطلَعين عند استلامهم رسائل من مصدر مجهول

يتناول هذا البند سلوكيات المستطلَعين عند استلامهم رسائل من مصدر مجهول (كان بإمكانهم اختيار أكثر من إجابة)، بيّنت النتائج أن السلوك الأكثر شيوعًا بينهم، أكثر من النصف (55.5%)، كان تجاهل الرسائل؛ ومنهم من اختار سلوكيات قد تُعتبر سلوكيات وقاية وحماية، على سبيل المثال الحذف مباشرة (32.5%) ومنع المرسل من التواصل نحو (13.2%)؛ وصرّح نحو (25%) منهم أنهم يفتحون الرسالة ويفحصون من هو المرسل.

قد يُعتبر تجاهل الرسائل مجهولة المصدر مسألة جيدة، بيد أنه فعل لم يُتخذ عن وعي وإدراك حول الجهات المُرسِلة أو طبيعة الاستهداف (أمني/ تجاري/ سياسي، اجتماعي). وإذا أخذنا بالحسبان احتمال أن يتكرر فعل إرسال رسالة من ذات الجهة، واحتمال أن يفتح المستخدم هذه الرسالة، فقد تكون العاقبة وخيمة؛ ولا سيما في ظل تطور أساليب الاحتيال والرقابة والاختراق. هذا المشهد إلى جانب ما طرحته المجموعات البؤرية يعزز ضرورة العمل على تدريب المستخدمين -على اختلاف مراحلهم العُمرية- بالطرق الفضلى للتعاطي مع الرسائل مجهولة المصدر.

10. الحماية الرقمية أثناء استخدام الإنترنت

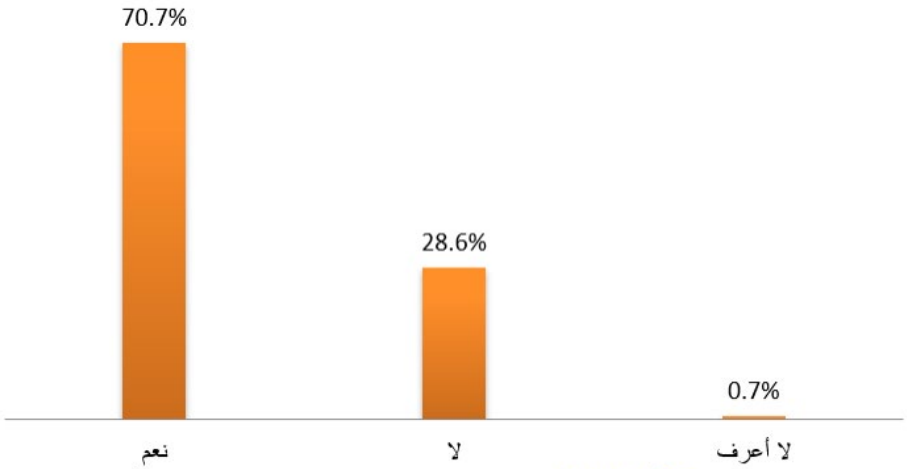


شكل رقم (15) توزيع أساليب الحماية التي يتخذها المستطلَعون أثناء تصفح الانترنت

تتلاءم الإجابات عن هذا السؤال مع إجابات المستطلَعين عن ما سبق من أسئلة تتعلق بالحماية والوقاية الرقمية. وتبيّن أن (78.5%) من المستطلَعين لا يستخدمون أي برامج أو وسائل للحماية؛ في حين يستخدم نحو 12% شبكة خاصة افتراضية "ڤي پي إن"[9]، و9.5% يستخدمون المتصفح الأعمى[10]، و3.9% من المستطلعين يستخدمون التشفير[11].

تعتبر الأرقام أعلاه صادمة نوعًا ما، ولا سيما أن المستخدمين لديهم معرفة حول المخاطر والتهديدات الرقمية، بيد أن هذه الأرقام لم تنعكس على الممارسة واستخدام الشبكة. وهي مسألة تعكس حالة من الاستهانة بالمخاطر الرقمية وحالة من انعدام الثقة، لا سيما إذا أخذنا بعين الاعتبار النقاشات في المجموعات البؤرية التي عبّر فيها المشاركون عن المخاطر التي تعرضوا لها من حسابات شخصية/وهمية.

11. خاصية تحديد الموقع الجغرافي



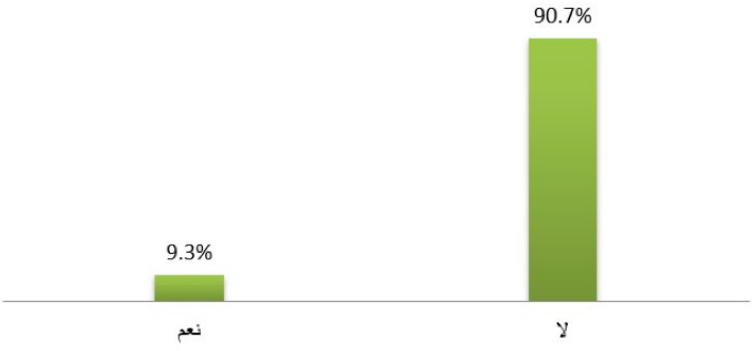
شكل رقم (16) نِسَب تشغيل خاصية تحديد الموقع الجغرافي بين المستطلَعين

تظهر النتائج أن ثلثي المستطلَعين (70.7%) يستخدمون خاصية تحديد الموقع الجغرافي، هذا يعني كشفهم للأماكن التي يتواجدون فيها. بينما صرح 28.6% منهم أنهم لا يستخدمون هذه الخاصيّة. يعزز هذا السلوك من مدى انكشافهم وافتضاح أمر أماكن تواجدهم، هذا السلوك قد تنتج عنه مجموعة كبيرة من المخاطر الرقمية (والفيزيائية)، ذات الأبعاد السياسية والاجتماعية، منها على سبيل المثال، استخدامه دليلًا للتهديد والاعتقال، إلى جانب تعزيز احتمالات انتهاك خصوصيتهم الرقميّة. ويعكس هذا السلوك غياب الوعي لدى فئات الشباب بخطورة تشغيل هذه الخاصية التي تتيحها الشبكات الاجتماعية من جهة، ومن جهة أخرى تتلائم هذه المعطيات مع المعطيات السابقة التي عكست نوع من القناعة السائدة بين المستطلَعين أنه لا جدوى من تفعيل أساليب الحماية.

9. ڤي پي إن ("VPN") يوفر امكانية الاتصال بالإنترنت دون الكشف عن مكان الاتصال.
10. المتصفح الأعمى يوفر إمكانية عدم تتبع وتقفي المواقع التي يتصفحها المستخدِم.
11. التشفير يوفر امكانية تحويل نص الرسائل إلى معلومات مشفرة بواسطة خوارزميات خاصة.

المحور الرابع: الهجمات والاعتداءات الرقمية

1. التعرض للإساءة أو للهجوم أو للابتزاز من متطفلين، أو مخترقين (هكرز)

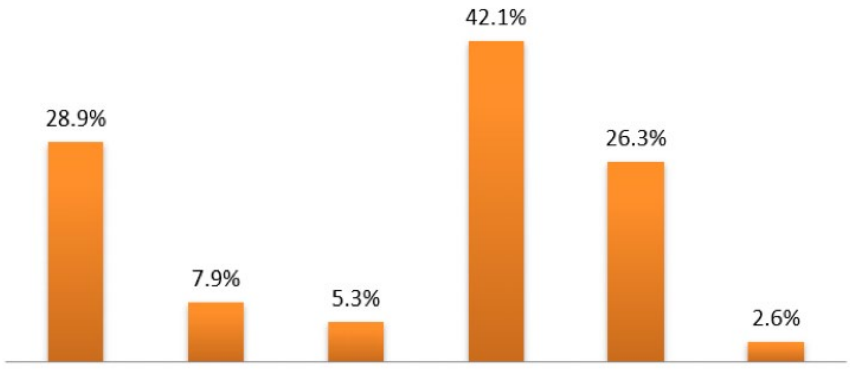


شكل رقم (17) نسبة المتعرضين للهجمات والاعتداءات الرقميّة

تُظهر النتائج أن الغالبية العظمى من المستطلَعين (90%) لم يتعرضوا لإساءات أو هجمات أو تهديدات أو اعتداءات أو ابتزازات رقمية من متطفلين أو مخترقين؛ في حين قال 9.3% من المستطلَعين أنهم تعرضوا لاعتداءات رقميّة.

لا يمكننا الاستخفاف بهذه النسبة مع أنها قد تبدو ضئيلة وهامشية للوهلة الأولى، إلا أنها مؤشر لمشاكل وسلوكيات مستخدمي الإنترنت مِن طرفي الهجوم -انظروا البندين التاليين- حسبما جاء في نقاشات المجموعات البؤرية. تشير نسبة الأفراد الذين تعرضوا للهجمات من عينة البحث إلى وجود مشاكل عميقة، مثل نقص الوعي والمعرفة في بعض الأحيان، وتجاهل التهديدات أو التعامل معها كأنها غير موجودة في أحيان أخرى، بالإضافة إلى الاستهانة بالهجمات الرقمية، مما يعكس عدم فهم المخاطر الرقمية وعدم اكتساب المهارات والممارسات الضرورية لحماية النفس في البيئات الرقمية. ووفرت النقاشات في مجموعات التركيز تفسيرا لهذه النسبة، فأغلب المشاركين عبروا عن تعرضهم لهجمات رقمية من متطفلين أو مخترقين، كان أبرزها التي جاءت على خلفية وطنية سياسية. لقد عكست الحوارات وشهادات المشاركات/المشاركين وتحديدا من فئات طلبة الجامعات والشباب وفئة الناشطات الحقوقيات تعرضهم لهجمات من مصادر اجتماعية وسياسية ودينية، فيما تضاعفت الهجمات وسياسات القمع الرقمي بعد الحرب على قطاع غزة.

2. أنواع الهجمات والاعتداءات الرقميّة

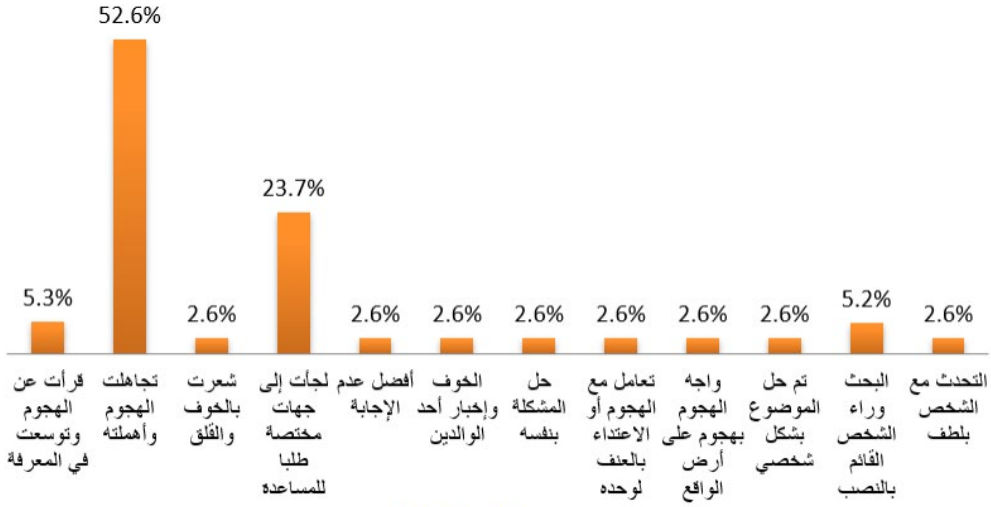


شكل رقم (18) أنواع الاعتداءات والهجمات التي تعرض لها المستطلَعون

حاولنا بواسطة المسح الميداني معرفة طبيعة ونوع الهجمات والاعتداءات التي تعرض لها المستطلَعين. في هذا البند قُدِّم لهم تعريف بسيط حول الإجابات المقترحة من أجل توحيد المفاهيم لدى المشاركين. أظهرت النتائج أن (42.1%) من الهجمات/ الاعتداءات كانت من نوع "انتحال الشخصية" – والمقصود: إنشاء حسابات تواصل اجتماعي وهميّة تستخدم اسم وصورة الشّخص المستهدَف، أو سرقة حسابات والسيطرة عليها. وكانت 28.9% من الهجمات من نوع هجمات "التصيد الاحتيالي" – المقصود: نوع من الجرائم الإلكترونية حيث يحاول المهاجمون خداع الأفراد للحصول على معلومات حساسة مثل أسماء المستخدمين، وكلمات المرور، وتفاصيل بطاقات الائتمان، وذلك من خلال التنكر ككيان موثوق به. عادةً ما يتم التصيد الاحتيالي عبر البريد الإلكتروني أو الرسائل النصية أو مواقع الإنترنت المزيفة. وكانت نسبة 26.3 % من الهجمات/الاعتداءات من نوع "التحرش والإساءة الرقميّان" – المقصود: استخدام الشبكات الاجتماعيّة استخدامًا عدائيًّا بهدف التنمّر والتهديد وإزعاج شخص ما، بواسطة التعليق على محتويات نشرها المعتدى عليه أو علّق عليها-. هجمات/اعتداءات من نوع "الترصد والملاحقة الالكترونية" – المقصود: مطاردة تشمل الاتهامات الكاذبة والتشهير والقذف، أو المراقبة أو نشر المعلومات الشّخصيّة الحسّاسة لشخص ما على الإنترنت- كانت بنسبة 7.9%. هجمات/اعتداءات اساءة استخدام الصور (البورنو الانتقامي) – المقصود: نشر صور أو مقاطع فيديو ذات محتوى جنسيّ صريح دون رضا الضحية التي تظهر في هذه المواد، أو نشر وتوزيع الصور والفيديوهات الحميميّة، الجنسيّة، أو الإباحيّة للأفراد دون موافقة منهم- كانت بنسبة 5.3%.

وتشير النتائج إلى بروز الهجمات المرتبطة بفئات "انتحال الشخصية"، "التصيد الاحتيالي"، و"التحرش والإساءة الرقميّان"، أما "الترصد والملاحقة الإلكترونية" فكان منفذوها حركات استيطانية يمينية متطرفة عملوا على إيذاء الفلسطينيين الناشطين سياسيا منذ الحرب على قطاع غزة. وأظهرت النقاشات مع المجموعات البؤرية تداخلا في الجهات التي تتسبب بالهجمات الرقمية ما بين الاجتماعي والسياسي والأمني، حيث هناك تداخل في طبيعة الجهات التي تنفذ الاعتداء وهو ما يضاعف التهديدات الرقمية، حيث لا توفر الشرطة الإسرائيلية حماية حقيقية كما أنه لا يتعامل مع الشكاوى بجدية كما قال المشاركون في النقاشات المعمقة.

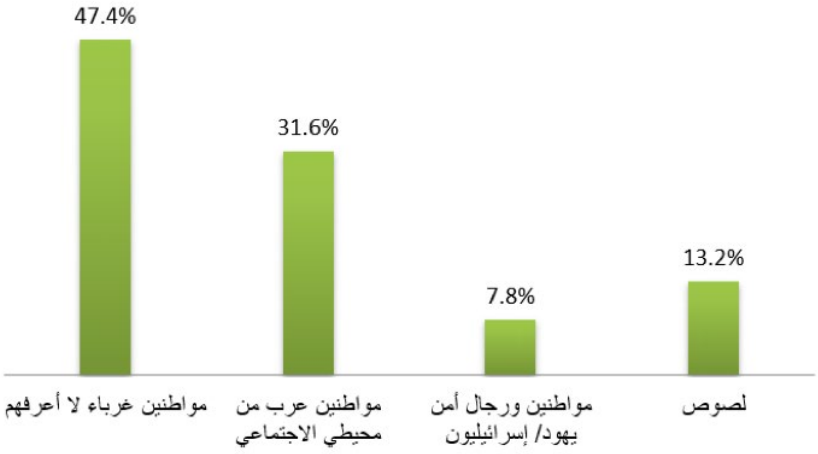
3. تعامل المستطلعين مع الهجوم أو الاعتداء الرقمي



شكل رقم (19) سلوك المستطلَعين بعد الهجوم الرقمي

تظهر النتائج (الشكل 19) أن رد فعل غالبية المستطلَعين الذين تعرضوا للهجوم هو تجاهل الهجوم وإهماله (52.6%)، بينما قال (23.7%) إنهم يلجأون إلى جهات مختصة طلبًا للمساعدة، وهناك من اختاروا القراءة وتوسيع معرفتهم عن الهجوم، وبلغت نسبتهم نحو 5%، نسبة مثيلة اختاروا أن يبحثوا عن الجهة وراء الهجوم. وتعكس النتائج أعلاه أن ثمة أزمة ثقة عميقة عند المستخدمين تجاه المؤسسات الرسمية وغير الرسمية – فقط ثلث المستطلَعين يلجأون لطلب المساعدة، وقد تكون أزمة الثقة هذه وانعدام الأجسام والمؤسسات الرسمية الداعمة هي الدافع لسلوك اللامبالاة الذي يتكرر في النتائج على طول الاستبيان. فغالبية الشباب لا يتخذون التدابير الضرورية عند البحث عن معالجة الاعتداء أو الهجوم الرقمي، وهو أمر كُشف عنه بوضوح نقاش المشاركين في المجموعات البؤرية.

4. الجهات خلف الهجوم أو الاعتداء

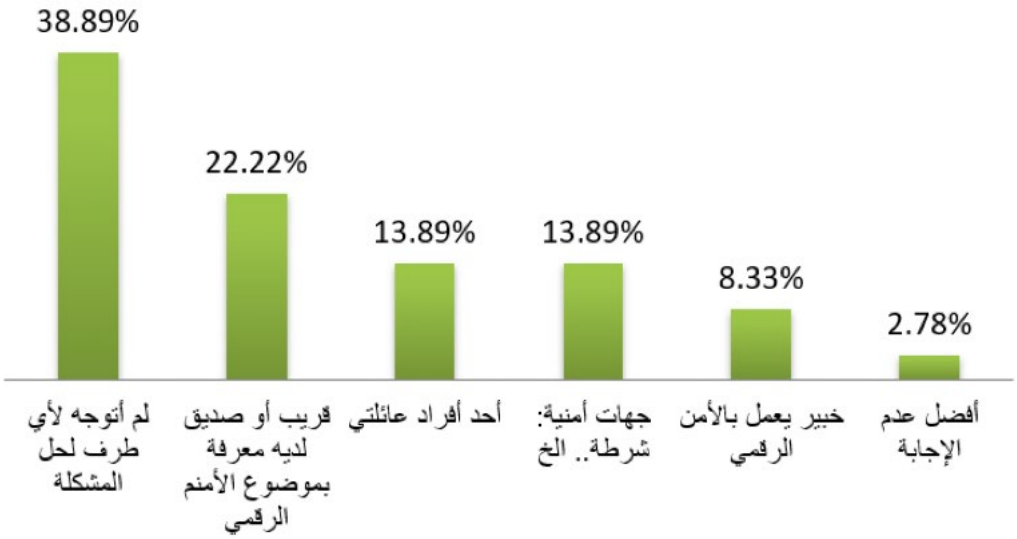


شكل رقم (20) الجهات التي تقف خلف الهجمات والاعتداءات الرقميّة

يظهر من النتائج (الشكل 20) أن نحو 47.4% من المعتدين كانوا أفرادًا مجهولين/غرباء بحسب أقوال المستطلَعين، بينما قال نحو 31.6% إن من اعتدى عليهم كانوا أفرادًا من محيطهم الاجتماعي؛ نحو 13.2% قالوا إن لصوصًا اعتدوا عليهم؛ أما الاعتداءات التي مصدرها مواطنين ورجال أمن إسرائيليين فكانت 7.8%.

عند قراءة هذه النتائج علينا الأخذ بالحسبان نتائج البند السابق لا سيما مجموعة المستطلَعين الذين يتجاهلون الهجوم والاعتداء الرقمي عليهم. فإذا كان المهاجمون أفرادًا مجهولين واخترنا تجاهل الهجوم فالاحتمال أن يكرر المهاجمون فعلتهم حتمي لأنه لم يبلَّغ عنهم. ولا يمكننا تجاهل نسبة من يتعرضون للاعتداءات من قبل أفراد من محيطهم الاجتماعي، فقد يكون هذا واحد من مسببات تعميق أزمة الثقة بين المستخدمين ومحيطهم.

5. الجهات التي لجأ إليها المستطلَعون بعد الهجوم أو الاعتداء الرقميّين



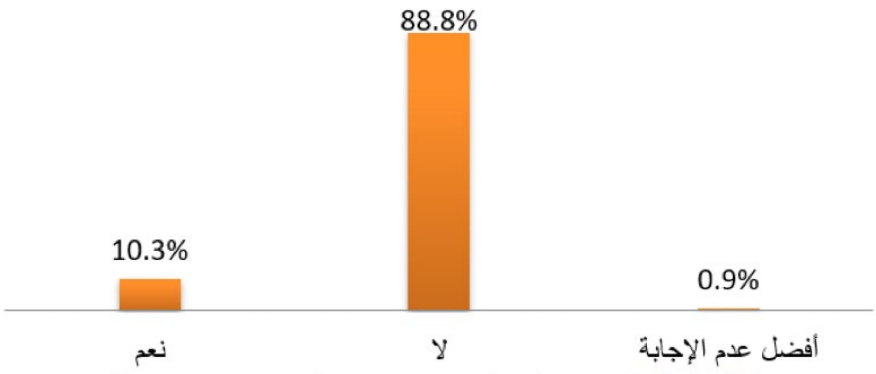
شكل رقم (21) الجهات التي يلجأ إليها المستطلَعون بعد التعرض لهجوم أو اعتداء رقميين

تُظهر النتائج (الشكل 21) أن 38.8% من المستطلَعين اختاروا التجاهل مرة أخرى ولم يتوجهوا لأي طرف لحل المشكلة؛ نحو 35% منهم يلجأون للدائرة القريبة (22.2% توجهوا لقريب أو صديق لديه معرفة بمسائل الأمان الرقمي، و 13.8% توجهوا لأحد أفراد العائلة)؛ ونحو 22% يتوجهون لجهات رسمية أو مهنية (13.8% يتوجهون لجهات أمنية وشرطية، و 8.3% يتوجهون لخبراء يعملون في مجال الأمان الرقمي).

مرة أخرى يختار المستخدمون الفلسطينيون في إسرائيل تجاهل المشكلة وحلها، أو يختارون التوجه للدائرة القريبة، هذه النتائج هي مؤشر آخر لعمق أزمة الثقة بين المستخدمين والدوائر الرسمية التي من المفترض أن تقدم يد العون في هذه الحالة، ومؤشر لمواضع ثقة الشباب الفلسطينيّين، ومؤشر للمؤسسات لضرورة التوعية في مجال الأمان الرقمي على المستوى الأسري. وقد دعمت النقاشات في المجموعات البؤرية هذه النتائج.

المحور الخامس: المساءلة والتحقيق من جهات أمنية

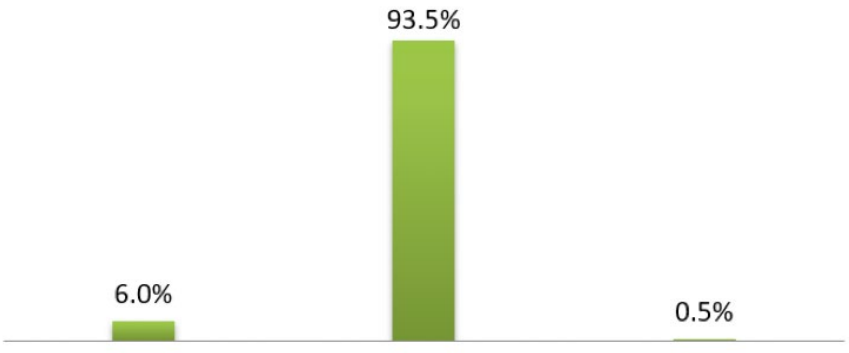
1. المساءلة أو التحقيق من قبل السلطات الإسرائيلية حول منشورات "التعبير عن الرأي"



شكل رقم (22) نسبة المستطلَعين (أو شخص يعرفونه) الذين أُستدعوا للتحقيق من جهات أمنية إسرائيليّة

يتبيّن من النتائج أن نحو 10.3% من المستطلَعين أو أحد أفراد محيطهم الاجتماعي أُستدعوا للتحقيق أو المسائلة من قبل السلطات الإسرائيليّة بسبب منشورات على منصات التواصل الاجتماعي. و88.8% منهم قالوا أنهم لم يُستدعوا للتحقيق أو المسائلة من قبل السلطات الإسرائيلية. وبالرغم من وجود فجوة كبيرة بين نسبة من استدعوا للتحقيق وبين من لم يتم استدعائهم، إلا أن الترهيب والملاحقة وتجربة التحقيق قد عززوا من الرقابة الذاتية المفرطة للأفراد الناشطين. ما برزن في النقاش داخل المجموعات البؤرية لاحقًا. ويرى الباحث أن النقاشات كانت في جو من الأمان والراحة التي جعلت من المشاركين يعرضون تجاربهم الخاصة أو تلك التي يعرفون عنها في محيطهم الاجتماعي، وكلها تعكس تزايد سياسات حكومة إسرائيل في استهداف النشطاء، وهو أمر يعزز من الخوف وعدم الأمان على خلفية النشر المرتبط بالتعبير عن الرأي السياسي وهو ما ساد بعد أحداث هبة الكرامة 2021، وتعزّز بكثافة منذ بدء الحرب على غزة بعد السابع من أكتوبر 2023.

2. ضغوط من دوائر اجتماعية لحذف منشورات تعبر عن آراء سياسية أو اجتماعية



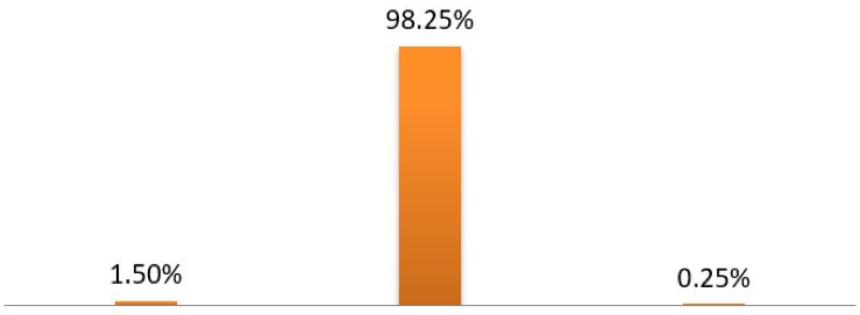
شكل رقم (23) التعرض لضغوطات لحذف منشورات سياسية أو اجتماعية

يظهر من النتائج (الشكل 23) أن 6% من المستطلَعين تعرضوا لضغوط من دوائر اجتماعية قريبة لمسح منشورات أو محتويات تعبر عن آراء سياسية أو اجتماعية، و 93.5% منهم لم يتعرضوا لمثل هذه الضغوط.

وأظهرت المجموعات البؤرية مؤشرات تتعارض مع هذه النتيجة نسبيا، حيث قال المشاركون في النقاشات أنهم يتعرضون لضغوطات دائمة من جهات اجتماعية (أب، أخ، عم، خال، قريب من العائلة) من أجل عدم التفاعل مع الأحداث السياسية والاجتماعية (جرائم القتل على سبيل المثال)، أو من أجل حذف منشورات على صفحات التواصل الاجتماعي.

ونقل المشاركين في المجموعات البؤرية تجارب تعكس استغلال أجهزة الأمن الإسرائيلية (الشاباك) طبيعة المجتمع الفلسطيني التقليدي الأبوي للضغط على نشطاء ومدافعات عن حقوق الإنسان من أجل قمع حرية التعبير عن الرأي في الأحداث السياسية أو في مجريات الحرب على غزة، وهو ما برز لدى الفلسطينيين من النقب، والناشطات في الدفاع عن حقوق الإنسان على العموم.

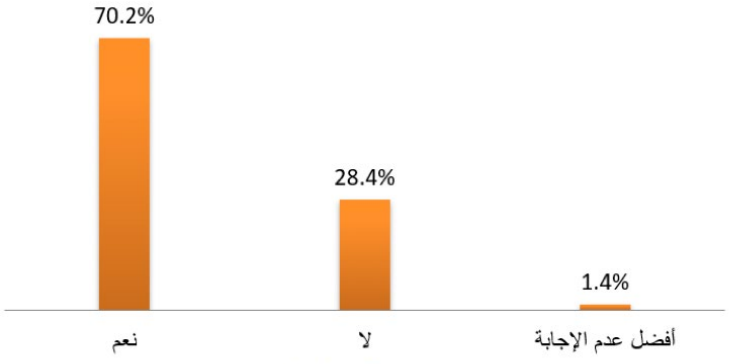
3. ضغوطات من دوائر أمن إسرائيلية لحذف منشورات أو محتويات سياسية



شكل رقم (24) التعرض لضغوطات أمنيّة إسرائيليّة لحذف منشورات سياسية أو اجتماعية

تُظهر النتائج نسبة من تعرضوا شخصيًّا لضغوطات أمنية إسرائيليّة مباشرة لحذف منشورات ذات طابع سياسي (1.5%) وقال (98.2%) أنهم لم يتعرضوا لأي ضغوطات أمنية إسرائيلية. يمكننا الاستنتاج من هذه النتائج أن المستخدمين يمارسون مستوى عال من الرقابة الذاتية على نشاطهم الرقمي كي لا يتعرضوا لأي ضغوطات وملاحقات أمنية إسرائيلية. يستوي هذا الاستنتاج مع ما صدر في مجموعات النقاش، حيث تعرض جانب كبير من المشاركين (باستثناء مجموعة طلبة المرحلة الثانوية) إلى ضغوط من دوائر أمنية. ويمكن الإشارة هنا إلى أن السلطات الأمنية الإسرائيلية أو مجموعات تضم نشطاء اليمين الإسرائيلي، مارسوا أساليب تخويف وتسببوا بإثارة القلق منذ بداية الحرب على غزة، بواسطة اعتقال أو استهداف مجموعة من الفاعلين والنشطاء في الداخل وهو ما أدى في نهاية المطاف لرقابة ذاتية عالية وقامعة. وقد مورست هذه الأساليب في أحداث هبة الكرامة 2021 كما قال أحد الشبان، وتعمقت في فترة الحرب على غزة. في البند التالي سنفسر جانبا من هذه النتائج.

4. الرقابة الذاتية

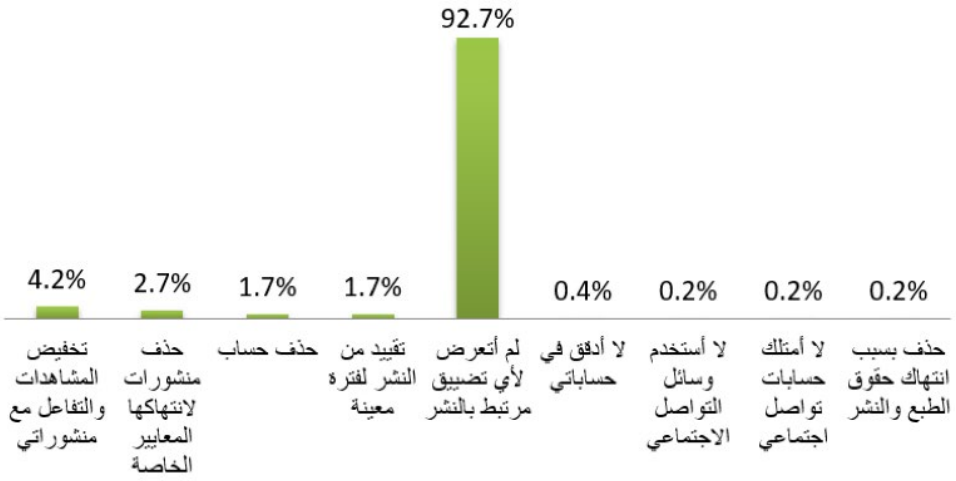


شكل رقم (25) مدى ممارسة الرقابة الذاتية

يتبيّن من النتائج أن نح 70% من المستطلَعين يمارسون رقابة ذاتية عند النشر على منصات التواصل الاجتماعي، بينما قال 28.4% أنهم لا يمارسون رقابة ذاتية عند النشر. وعلى ما يبدو أن هذه النتائج هي حصاد سياسات القمع الرقمي والضغط الأمني والاجتماعي التي خلقت أزمة ثقة عميقة رأينا عوارضها وتأثيرها في البنود السابقة. عززت النقاشات في المجموعات البؤرية هذه النتائج، إذا جاء على لسانهم أنهم غالبًا ما يمتنعون عن الكتابة والنشر والتفاعل في ظل سياسات التخويف والملاحقة والقمع الرقمي التي تمارسها إسرائيل الرسمية وغير الرسمية.

المحور السادس: أثر سياسات منصات التواصل الاجتماعي على نشاط الشباب الفلسطيني منذ بدء الحرب على قطاع غزة

1. تقييدات فُرضت على الحسابات من قبل شبكات التواصل الاجتماعي



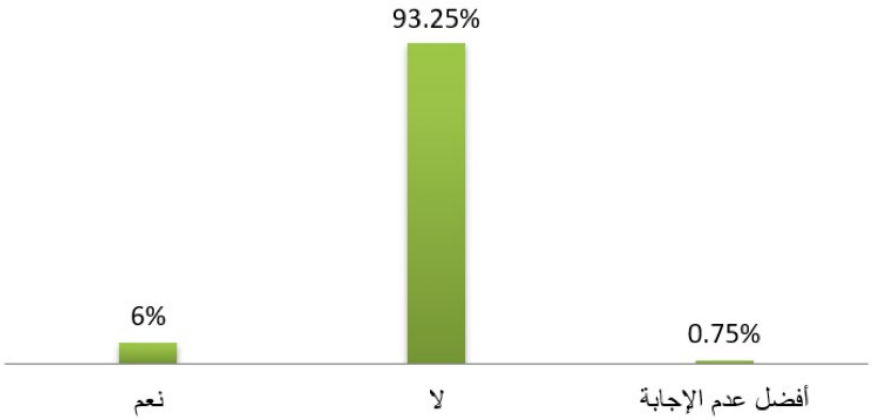
شكل رقم(26) أنواع التقييدات التي فُرضت على حسابات المستخدمين الشخصية من قبل شبكات التواصل الاجتماعي

خُصص هذا السؤال (الشكل 26) للتقييدات التي تعرضت لها حسابات المستخدمين في الشهور الثلاثة الأولى من بدء الحرب على غزة، وكان على المستطلَعين أن يختاروا نوع التقييدات التي فُرضت على حساباتهم. وتبين النتائج أن 92.7% منهم لم يتعرضوا لأي تقييد أو حذف؛ و4.2% منهم قالوا إن منشوراتهم خضعت لتقييدات في الوصول لشريط الأخبار والأصدقاء؛ و2.7% قالوا إن منشوراتهم حُذفت بادعاء انتهاك معايير المنصات وسياساتها.

تشير هذه النتائج إلى تأثير السياسات القمعية التي تتبعها الحكومة الإسرائيلية، والتي تؤدي إلى فرض رقابة ذاتية على تفاعل المواطنين مع الحرب على غزة. يظهر أن الفلسطينيين في الداخل لم يواجهوا قيودًا تتعلق بالنشر أو الوصول إلى منصات التواصل الاجتماعي، كما هو الحال مع الفلسطينيين في الضفة الغربية والقدس، ويرجع ذلك إلى عدم تفاعلهم مع الأحداث.

وتخلص النقاشات في المجموعات البؤرية إلى استنتاجات مهمة تشرح وتفسر تلك النتائج وتؤكد عليها، فمن ناحية أولى ترتب على الشباب في الداخل أن يستخدموا المنصات والشبكات الاجتماعية من أجل متابعة الأخبار فقط وليس التفاعل معها، (فهم يعيشون في وسط عام: الجامعة، العمل، يمنعهم من التعبير عن مشاعرهم)، فيما أكد جانب من المشاركين والنشطاء أنهم توقفوا عن التفاعل في حساباتهم أو أغلقوها بعد الحرب على غزة مخافة أن تستخدم ضدهم في ظل حملات الاستهداف والتصيّد التي شنّها الإسرائيليّون.

2. تقييدات النشر على المنصات وأثرها على التفاعل مع الأحداث السياسية



شكل رقم (27) مدى تأثير تقييدات النشر على التفاعل مع الأحداث السياسية منذ البدء الحرب على غزة

بهدف معرفة أثر القيود الرقمية التي فرضتها المنصات على المستطلَعين قُرأت عليهم المقولة التالية: "تعرضت حساباتي على شبكات التواصل الاجتماعي إلى تضييق مرتبط بالنشر وهو ما قلل من تفاعلي مع الأحداث السياسية المختلفة، خلال الشهور الثلاثة الماضية" (بعد 7 أكتوبر 2023). اتفق 6% منهم مع المقولة، فيما أجاب نحو 93.2% بـ"لا".

وتمنح النقاشات مع المجموعات البؤرية إشارات مهمة لفهم هذه النتيجة التي تبدو مخالفة للتوقعات، حيث قال المشاركون إنهم لم يتفاعلوا مع الأحداث في غزة إلا في أضيق نطاق، وقد اقتصر نشاطهم على نشر بعض المنشورات الإنسانية، ومع ذلك عرضتهم للمساءلة والملاحقة أيضا؛ وشدد بعض المشاركين على أنهم أحجموا عن أي مشاركة أو تفاعل سياسي ووطني رغم طبيعة مشاعرهم الوطنية التي كانت تشعرهم بالغضب والإحباط وعدم القدرة على العمل والتحرك.

ثانيا: نتائج المجموعة البؤرية الخاصة بالناشطات في مجال حقوق الإنسان

ضمت مجموعة التركيز المتعلقة بالمدافعات عن حقوق الإنسان في الداخل ست ناشطات في مجال حقوق الإنسان. توزعت مِهنهنّ على النحو التالي: محامية؛ مُتطوّعة في جمعيّة ثقافية واجتماعية؛ مركّزة إعلام في جمعيّة إغاثة؛ موظفة في مؤسسة تُعنى بقضايا الإنترنت وحقوق الإنسان؛ صحافيّة؛ عضوة في الحزب الشيوعيّ؛ ناشطة شبابيّة؛ متطوّعة في عدّة مؤسسات حقوق إنسان. استمر النقاش مع الناشطات 3 ساعات، وتمحور حول النقاط التالية: واقع استخدام الناشطات للإنترنت وللشبكات الاجتماعية؛ مدى معرفتهن بالأمان الرقمي؛ دور المؤسسات التي يعملن بها في توفير حماية رقمية لهن؛ ومصادر الانتهاكات للحقوق الرقمية وطبيعة الهجمات التي تعرضن لها؛ وتأثير الحرب على قطاع غزة على نشاطهن الرقمي.

وهدفَ النقاش في المجموعة الوقوف على مدى معرفة ناشطات حقوق الإنسان بموضوع الأمان الرقمي بكل ما يتعلق بعملهن ونشاطهن، من أجل توفير سبل وقاية وموارد تضمن سلامتهن وتمنع المخاطر والانتهاكات الرقمية ضدهن، ومن أجل العمل على تعزيز شرعية عملهن عبر سن قوانين ووضع سياسات، ولا سيما أنهن ينشطن في أوقات الأزمات وفي مناطق الصراع. فيما يلي أبرز ما ورد في النقاش:

ناشطات أكثر حذرًا في سرد تجاربهن الرقمية

برز في النقاش الحذر الشديد في كشف تفاصيل تجارب المشاركات الشخصية، إذ شددن على أهمية عدم ذكر أسمائهن أو المؤسسات التي يعملن بها، أو أي ملمح يمكن أن يدلل على هويتهن. علاوة على ذلك، فهن لم يعرضن كامل تجاربهن في البيئة الرقمية (خلال النقاش)، على الرغم من تأكيدهن على أنهن تلقين تهديدات وهجمات متنوعة في العالم الرقمي والواقعي الذي كن يتواجدن فيه بكثافة، مما أدى إلى انحسار نشاطهن الرقمي وتفاعلهن مع القضايا الحقوقية المختلفة، وهو ما تضاعف بعد أحداث الحرب الإسرائيلية على قطاع غزة.

ناشطات يفقدن الأمل في التغيير

عكست النقاشات العميقة مع المشاركات أنهن في حالة من فقدان الأمل الشديد فيما يتعلّق بإيمانهن بقدرتهنَّ على التغيير السياسي والاجتماعي، إلى جانب شعورهنَّ بالإحباط العام، وقلّة الحيلة، وأحيانا القهر، والعجز والغضب أمام الظروف السياسية والاجتماعية والثقافية والحقوقية التي يعشن في ظلها في الداخل، وهو ما انعكس على تواجدهن المباشر على شبكة الإنترنت وعلى المنصات الاجتماعية، وانعكس كذلك على التفاعل على المنصات مع القضايا الحقوقية والاجتماعية والسياسية.

اعتداءات رقمية كثيرة وجهات متنوعة تقف خلفها

أظهرت النقاشات مع المدافعات أن هناك تنوعا في الجهات التي تقف خلف الاعتداءات الرقمية أو الضغوط والتهديدات الرقمية التي تعرضن لها، فعلى سبيل المثال، تشمل هذه الجهات، الأحزاب السياسية العربية التي سعت إلى قمع الناشطات لمنعهن من توجيه النقد إليها؛ أعضاء ورُؤساء أو مُرَشّحي مجالس محلية في المدن والبلدات العربية؛ تهديدات وضغوطات مصدرها أشخاص ينتمون لعائلات كبيرة (في حال طال النقد وجهاء العائلات)؛ إلى جانب الاعتداءات الرقمية التي مصدرها الحكومة الإسرائيلية ومُؤسساتها وأذرعها الأمنية؛ وأخيرًا، مجموعات المستوطنين الإسرائيليين العنصرية التي تقوم بمراقبة حسابات الناشطات والتربص لهن وتهديدهن باستمرار. وعلى الرغم من أن هذه الممارسات قد ازدادت بشكل كبير بعد الحرب على قطاع غزة، مما خلق أجواءً من القمع والخوف، إلا أنها كانت موجودة أيضًا قبل الحرب ولكن بنسب أقل.

وأظهرت النقاشات أنه ثمة ما هو مشترك في مصادر الضغط على الناشطات، إذ تلجأ هذه المصادر إلى دوائر اجتماعية قريبة منهن (أب، أخ، عم، خال، كبير عائلة) من أجل حذف منشورات، وتخفيف حدة الانتقادات، أو عدم التعبير عن الرأي في البيئة الرقمية وصولًا إلى عدم المشاركة في أنشطة سياسية وحقوقية في الميدان.

وأشارت المشاركات إلى وجود تدخّلات واسعة وكثيرة من المجتمع بشأن ما ينشرنه، وتشكيك في غاياتهن من وراء هذه المنشورات أو ما يتفاعلن معه، فضلًا عن اعتبار آبائهنَّ جسمًا سلطويًّا ومسؤولًا عنهن، بل ومُخوَّلًا بفرض القيود والسيطرة عليهن. لذلك، غالبا ما كانوا يتوجهون إلى (الآباء) بشأن تعبيراتهنالرقميّة، ومطالبته بمُساءَلَتِهنَّ، وجعله جسرا لتوصيلَ التحذيرات لهُنَّ وبالتالي عملية قمعهن التي تشارك بها أطراف كثيرة داخل الدائرة الاجتماعية القريبة منهن. تقول إحدى المشاركات:

> "تحذيرات المجتمع تضاعفت: كان يتمّ تحذيري من ناس اللي هُمّي مُقرَّبين، وحتّى ناس بعيدة اللي كانت تِسمَح لحالها تصل لمُقَرَّبين لإلي، وإنّه خلّيها تنتبه مثلًا... مثلًا بنزّل صورة العلم الفلسطينيّ كان يتم التحذير.."

وفي جانب آخر، بَرَزَت في الحوار مع الناشطات قصصا للهجوم عليهُنَّ من قبل رجال أصحاب قُوَّة ومناصب عليا، أو شخصيات عامة لديها قاعدة جماهيريّة واسعة في المجتمع، وهو أمر وصل حد الطلب من مؤيدي الشخصيات العامة مهاجمة الناشطات الحقوقيات.

قيود رقمية على خلفية جندرية

ترى المدافعات عن حقوق الإنسان أن نسبة كبيرة من الاعتداءات الرقمية والضغوط التي يتعرضن لها تعود أساسًا لأسباب تتعلق بالنوع الاجتماعي (الجندر). يمنح المجتمع الرجال السلطة والشرعية لانتهاك حقوق النساء واستضعافهن فقط لكونهن نساء، وذلك على اختلاف القضايا التي يتحدثن عنها، وأحيانًا بسبب فئتهن العمرية (لكونهن ناشطات شابات)، أو بسبب تصنيفهن الاجتماعي (أمهات، مطلقات..).

تراجع استخدام المنصات وصولا إلى حذف الحسابات

أظهرت النقاشات أن هناك تنوعا في مصادر الاعتداءات الرقمية (سياسيا واجتماعيا ودينيا..الخ) وهو ما ترك أثرا سلبيا على جميع الناشطات المشاركات، إذ سادت حالة من العزوف عن استخدام المنصات الرقمية وشبكات التواصل الاجتماعي، وهو ما ترجم في ضعف حضورهن في البيئة الافتراضية مقارنة بسنوات سابقة، وعكست النقاشات أن هناك تراجعا كبيرا في شعورهن بالأمان الرقمي وضمان حقوقهن الرقمية في ظل الحالة التي تعيشها البلاد (الحرب على قطاع غزة). فيما رأت بعض الناشطات أن المساحة الحرة التي كانت تتيحها هذه المنصات تراجعت كثيرا وصولا إلى الحرب على قطاع غزة، حيث أصبح كل ما ينشرنه مصدرا للتهديد والملاحقة والاعتقال والاغتيال المعنوي من أجهزة الدولة أو من جماعات عنصرية متطرفة تلاحق العرب الفلسطينيين والنساء الناشطات بشكل خاص.

الحرب على غزة علامة فارقة على الاعتداءات الرقمية

أجمعت الناشطات خلال المحور الثالث من النقاش (معرفة الأمان الرقمي وإدراك المخاطر الرقمية) أن الحرب على قطاع غزة والمخاوف التي صعدت مع اندلاعها شكلت علامة فارقة على نشاطهن وتعبيرهن عن ذواتهن. استخدمت جميع الناشطات كلمات "قبل الحرب شي وبعد الحرب شي آخر"، دون أن يعني ذلك أن ما قبل الحرب أفضل كثيرا. لكن الثابت بالنسبة للناشطات أن المخاطر تضاعفت بعد الحرب والإحساس بالأمان الرقمي أصبح مفقودًا تماما في ظل المشاهد التي كانت تأتي من القطاع والمخاوف التي عززتها التهديدات التي أطلقتها أجهزة الدولة الامنية والاعتقالات التي نُفذت بحق شخصيات معروفة لكونها نشرت «منشورًا" واحدًا. فالملاحقة والخوف من المشاركة في الاحتجاج ضد الحرب في الميدان انعكس بعمق على البيئة الرقمية وعلى أحاديث المواطنين الحقوقية، وعبرت بعضهن عن ملاحقة أمنية ومطاردة وتتبع ومراقبة رقمية حتى على التعليقات التي كان يكتبها طواقم عمل في المؤسسات، كما حذفت بعض المؤسسات قوائم بأسماء الموظفين فيها عن شبكة الإنترنت مخافة أن يُلاحقوا ويُراقبوا من جهات أمنية أو متطرفين لكونهم يعملون في مجال الدفاع عن حقوق الفلسطينيين. تقول إحدى الناشطات:

> "أنا كُل يُوم بفيق حرفيًا بتطلّع عالأخبار إذا طلع التقرير عنّي (مواد تشهيريه على الشبكة). مش بس عنّي بشكل خاص، كمان عن الموظفين اللي بشتغلوا معي، طلعوا تقرير قاتل عن المُدير اللي عنّا، قالوا: ليش بعدوا عايش؟ حرفيا. إنّه ليش هذا الإنسان بعدو عايش؟ وانتشر التهديد كثير. وانتشرت صورنا كموظفين على الشبكات. وانتشرت كثير تفاصيل عنّا. وبفكّر إنّه الإشي كثير صار مُرعب".

مؤسسات لا توفر الحد الأدني من الأمان الرقمي

أظهر النقاش مع مجموعة الناشطات أن جانبا كبيرا من المؤسسات التي يعملن بها لا توفر حدًّا أدنى من معايير الأمان الرقمي لضمان الحفاظ على سلامة الناشطات، بينما أكدت أخريات أن المؤسسات التي يعملن بها وضعت ما يشبه السياسات للتعامل مع التهديدات الرقمية وتحديدًا بعد الحرب على غزة، من ضمنها مجموعة من المعايير الرقمية لضمان حدًّا أدنى من الأمان للعاملين، لبياناتهم، ولمن يتلقون خدمات منها. إلى جانب ذلك قالت بعض الناشطات إنهن يفصلن بين عملهن ونشاطهن الحقوقي الرقمي والتعبير عن وجهات نظرهن الخاصة وبين عملهن في المؤسسات المختلفة.

تراجع في رأس المال الاجتماعي الافتراضي

عكست شهادات الناشطات حالة يمكن أن يطلق عليها تراجع رأس المال الاجتماعي الافتراضي على الشبكات، ويقصد بذلك تراجع درجة الثقة والتضامن ما بين الناشطة والأصدقاء والمتابعين لحسابها. أزمة الثقة هذه دفعت ببعضهن إلى حذف مئات الأشخاص الذين كانوا بمثابة "أصدقاء" أو الغاء متابعة المئات، وفي أحيان أخرى إغلاق الحساب. تقول إحدى المشاركات:

"الشي اللي زايد هاي الفترة هو عدم الثقة، يعني خلال فترة الحرب، أنا كان عندي الإنستغرام، بس لمّا شُفت، يعني أوّل ما شُفت الملف، (تقرير تحريضي يرصد تعليقات الناشطات) إنّه تمّ تعقُّب صبايا وشباب فيو. يعني كانوا يحطوا شو البوستات اللي طلعوها في 7 أكتوبر، الخوف تضاعف، شو يعني الخوف تضاعف. عدم الثقة يعني إنّه الناس أنا دُغري انتبهت إنّه أغلب الستوريز المأخوذة هي من الكلوز فريندز. فكان هذا عندي الإشي هيكا كمان صعب".

ومن تجربة ناشطة أخرى:

"وقت ما تمّ الحُكم على أدهم بشير (ناشط شبابي حكم على خلفية أحداث هبة الكرامة)، أنا نزّلت بوست إنّه الدولة تصدر هذه الأحكام كأداة ردع، وقتها كان في حساب كاين عاملي له "Follow". وراح عمل "Screenshot"، ونزّلها على التويتر. اسا طبعًا المُجتمع الإسرائيليّ فعّال جِدًّا على التويتر يعني، وبدأ الهجوم علي من نشطاء اليمين.. وقتها عنجد أنا خفت. أوّل إشي غيّرت اسمي على الإنستغرام. إنّه هو صوّرني إشي وغيرته. غيّرت بروفايلي. غيّرت كل شي. يمكن حتّى يوميتها لغيته لأسبوع، بس تخفّ الهجمة.. دخلت بحالة خوف.. مسبات وشتائم ودعوات للطرد".

تنامي حالة عميقة من الرقابة الذاتية

أظهر النقاش داخل المجموعة تصاعدًا ملحوظًا في حالة الرقابة الذاتية، فرغم أن الناشطات حقوقيات أو لديهن معرفة بحقوقهن إلا أن هناك رقابة ذاتية مضاعفة تجعلهن يكتبن المنشور أو التعليق ومن ثم يحذفنه مباشرة، تقول إحداهن:

"يعني مرّات بنزّل بُوست مثلًا ناقد أو إشي، بوخدش دقيقة. بمحاه خلص. بدّيش أشارك".

ويُلحظ ذلك حتى في أكثر القضايا التي تمس النساء في الداخل، قضايا القتل وتحديدا قتل النساء، حيث يحجمن عن التعبير عن وجهات نظرهن في ظل ما يطالهن من تهديدات. وظهر في النقاشات أن تجارب القمع الرقمي والاعتداءات الرقمية في السياق الاجتماعي والسياسي، تركت أثرها على تجارب النساء وموقفهن من المسائل الحقوقية التي يُفترض أن يدافعن عنها. فيما تتضاعف الرقابة الذاتية مع زيادة إحساس الناشطات بإنهن مراقبات في بيئاتهن الرقمية، حيث أصبحن يشعرن أنها مساحة تفتقد الأمان، على اختلاف الجهات المتسببة بذلك. تقول إحدى المشاركات:

"حتّى إنهن كانوا يراقبونا كمُوظّفين على تعليقاتنا، على عائلاتنا، على مين أصحابنا؟ شو توجّهات أصحابنا؟ لهاي الدرجة كان في ملاحقة صراحة. فصُرنا أكثر حذرين في التعليقات عند بعض، في حكينا. بتعرفي توعية بتعليمات من المؤسسة".

وتقول مشاركة أخرى:

"بحكولي إنّه التيلغرام مش مراقب بتقدري تحكي عادي. بس انا ما بسترجي.. يعني لهاي الدرجة. إحنا خايفين إنه إحنا مراقبين، ويمكن إحنا عنجد مراقبين، أو 100% مُراقبين... قسم كثير من الأشخاص اللي عندي على المنصة محيتهن. كمان بخاف أعلّق عند الناس اللي لسه عندي ع الفيس بوك. باجي بدي أكتب الكومنت، وبّدي أنشره، بس بعدها بمحاه".

مجتمع غير مرئي وناشطات غير مرئيات

ركزت الناشطات على أنهن ينظرن إلى الفلسطينيين في الداخل على أنهم غير مرئيين بالنسبة للدولة ومؤسساتها المختلفة، وهذا ينعكس على مطالبهن وواقعهن، إنهن غير مرئيات Invisible. وهذا ما دفعهن لطرح أسئلة حول جدوى صُراخهن وتعبيرهن عن اضطهادهن وظُلمهن في البيئات الرقمية. وقد تميّز حديثهن عن مقاربة مدى شرعية الحديث عن همومهن ومعاناتهن كناشطات بالمقارنة مع ما يجري في قطاع غزة بحساسية عالية، لأنه لا يمكن مقارنة الهموم بين المكانين في ظل حرب الإبادة الممارسة ضد الفلسطينيين في القطاع.

وخلصت المشاركات أنه يُمكن القول إنّ محو تجارب الفلسطينيّين في الداخل وقمع الانكشاف visibility الخاصّ بهم، يكون من خلال الفرد الفلسطينيّ نفسه، القمع الرقمي الذاتيّ الذي مصدره الجماعة الفلسطينية، والآخر الإسرائيلي الذي ينقسم إلى قمع الدولة وأجهزتها الأمنية الممأسس، من خلاله تحاصر النساء فيمارس قمعًا ورقابة عليهن، والقمع الآخر من الإسرائيلي المتطرف الذي يراقب ويتابع ويشن الهجمات المختلفة على الناشطات في ظل تصاعد خطاب اليمين الإسرائيلي المتطرف.

ملخص ونقاش النتائج العامة

تسلط هذه الدراسة الضوء على مفهوم الأمان الرقمي في الداخل بواسطة تقفي آثار تجارب مستخدمي شبكة الإنترنت الفلسطينيّين. جاءت هذه الدراسة في مرحلة غاية في الحساسية والاضطراب والتحوّل، وبغية استخلاص استنتاجات ذات مصداقية استخدمت الدراسة طريقتين لجمع البيانات وهما: المجموعات البؤرية، والمسح الميداني (استطلاع الرأي).

- أظهر الإطار النظري للدراسة قلة الأبحاث والدراسات حول تجارب مستخدمي شبكة الإنترنت الفلسطينيّين مواطني دولة إسرائيل. تتعامل معهم الدراسات المتوفرة على أنهم جزء من المجتمع الإسرائيلي، أو جزء من الشعب الفلسطيني، دون أخذ خصوصية مواطنتهم ووطنيتهم بعين الاعتبار، ولا سيما في ظل تداخل السياسات وتضاربها وبالتالي تأثيرها على استخداماتهم لشبكة الإنترنت ومنصاتها.

- بيّنت الدراسة أن دولة إسرائيل طورت من منظومة سيطرتها على استخدامات شبكة الإنترنت ومنصاتها من خلال تطوير منظومة قانونية وتعليمات وسياسات متناغمة، نتج عنها انتهاكات شديدة للحقوق الرقمية، واستطاعت أن تخلق حالة من "الرعب الرقمي" دفعت بقطاع الشباب إلى الإحجام عن التعبير عن الرأي والتفاعل مع قضايا وطنية وسياسية، إلى جانب استغلال أنظمة اجتماعية تقليدية وبنى ذكورية من أجل السيطرة والتحكم والقمع.

- بيّنت النتائج أن مستخدمي الإنترنت يفضلون استخدامه في المنزل على باقي الأماكن (المقهى، الجامعة، الحيز العام)، وقد تكون هذه النتائج مؤشرًا لحالة عدم الإحساس بالأمان الرقمي وانعدام الثقة السائد بين مستخدمي الإنترنت من فلسطينيي الداخل.

- أشارت النتائج أن نحو نصف المستخدمين يقضون ما بين 9-4 ساعات يوميا على شبكة الإنترنت، وتتركز معظم استخداماتهم للإنترنت، لا سيما على شبكات التواصل الاجتماعي، في استهلاك الأخبار، بينما تراجع تفاعلهم ونشاطهم في مواضيع سياسية وقانونية وحتى اجتماعية تراجعًا بارزًا. يمكننا اعتبار هذا السلوك علامة من علامات أزمة الثقة والرقابة الذاتية التي يعيشها مستخدمي الإنترنت من فلسطينيي الداخل.

- تبيّن من النتائج أن غالبية المشاركات والمشاركين يستخدمون أكثر من شبكة اجتماعية وتطبيق للمراسلة معظمها بحوزة شركة ميتا، وبعضها يسهل عملية الاختراق والرقابة والملاحقة. تفوّق تطبيق المراسلة والتواصل واتس اب على باقي التطبيقات، تلاه تطبيق انستغرام تلته منصة فيسبوك ومن ثم تطبيق تيك توك وتلغرام على التوالي.

- رأينا في بعض النتائج تناقضات، فعلى الرغم من أن ثلثي المستطلَعين على معرفة ودراية في برامج التجسس ومخاطرها إلا أنهم لا يأبهون بها وغير مبالين تجاهها، ولا يمارسون سلوكيات تحميهم من هذه المخاطر، مثل تغيير كلمة المرور بوتيرة عالية أو تحديد الموقع الجغرافي أو مشاركة الصور والأمور الشخصية على سبيل المثال.

- ومن التناقضات التي لمسناها، أن المستطلَعين على الرغم من معرفتهم بالمخاطر وعلى الرغم من معرفتهم بأساليب الحماية إلا أنهم لا يثقون في برامج الحماية ومصادرها. هذا السلوك إن دلّ على شيء فهو يدل على عمق انعدام الثقة لديهم، وقد تكون هذه الحالة من انعدام الثقة مشتقة من الوضع العام والسياقات السياسية والاجتماعية المختلفة التي يعيشون في كنفها.

- وكانت أكثر النتائج غرابة هي حالة اللامبالاة والاستهانة بالمخاطر التي من المحتمل أن يتعرضوا لها على اختلاف مصادرها وتنوعها. لم تقتصر مصادر الضغط والملاحقة على الدولة وأجهزتها وإنما تشارك في هذا الفعل الأحزاب السياسية ورجالات الأعمال وأفراد العائلة.

- وبحسب النتائج، ثمة حالة سائدة من التجاهل واللامبالاة في التعامل مع مصادر التهديد والخطر، ولا سيما تجاهل الرسائل مجهولة المصدر، وعدم التدقيق في الجهات التي أرسلتها. تعكس هذه حالة سلوكًا سلبيًا على مستوى المعرفة والوعي والممارسة أيضا.

- بعد الحرب على قطاع غزة تضاعفت الهجمات وسياسات القمع الرقمي، وبرزت الهجمات والاعتداءات على خلفية سياسية ووطنية، وقد وقفت خلفها جهات سياسية ودينية واجتماعية، بحسب أقوال المشاركات والمشاركين في المجموعات البؤرية. وكانت أبرز أنواع الهجمات والاعتداءات "انتحال الشخصية"، "التصيد الاحتيالي" و"التحرش والإساءة" (انظروا الشكل 18). وقد تحمل هذه النتائج بعض التفسير لأزمة الثقة التي يعاني منها المستخدمون، إذ أن الأطراف التي يمكن الاعتماد عليها واللجوء لها عند الضرورة أصبحت مصدر قلق وترهيب.

- وكان "التجاهل" هو السلوك الأبرز في تعامل الشباب من فلسطينيي الداخل مع الاعتداءات الرقمية، أي إهمال الهجمات الرقمية وعدم متابعتها. يمكننا اعتبار هذا السلوك مؤشرًا جِدّيا لأزمة الثقة التي يعيشها الشباب، فهم يفضلون السكوت والتجاهل والمعاناة لأن ليس لديهم جهة رسمية أو مهنية يثقون بها.

- لا يمكننا قراءة النتائج بمعزل عن سياسات القمع والملاحقة التي مارستها دولة إسرائيل بأجهزتها الأمنية والقضائية على الناشطات والناشطين في السنوات الأخيرة، لاسيما بعد هبة أيّار 2021 ومنذ بدء الحرب على قطاع غزة في العام 2023. تعكس البيانات التي حصلنا عليها مشهدًا مروعًا من الرقابة والقمع الذاتيين، فقد فضّل الشباب استخدام الإنترنت الصامت، أي الاكتفاء بمراقبة الأخبار ومجريات الأحداث دون التفاعل معها. ولكن حتى هذا الاستخدام تحاول الحكومة الإسرائيلية السيطرة عليه من خلال سن قوانين تراقب المواقع التي يتردد عليها الفلسطيني لتسهيل ملاحقته وتجريمه.

- نقلت المشاركات في المجموعات البؤرية تجارب تُبيّن استغلال أجهزة الأمن الإسرائيلية (الشاباك) طبيعة المجتمع الفلسطيني التقليدي الأبوي للضغط على ناشطين وحقوقيات للحد من تعبيرهم عن آرائهم حول الأحداث السياسية أو حول مجريات الحرب على غزة، وقد برز هذا في تجارب الفلسطينيين من النقب، والناشطات في الدفاع عن حقوق الإنسان.

- برزت مجموعة من الفروق الجندريّة في شعور الأمان الرقميّ بين الشباب والشابات بسبب طبيعة وأعراف المُجتمع البدويّ المُحافظ في النقب، في ظل أنماط المعيشة واتّباع نظام العشائر، لكن تلك الفروق تراجعت لصالح استخدام المنصات والتواجد على الشبكة بشكل عام.

- في المجموعة البؤرية الخاصة بالناشطات في مجال حقوق الإنسان تبيّن أنهن تعرضن لضغوط واعتداءات رقمية على خلفية نشاطهن الحقوقي على الشبكة، في حين شهدت مظاهر القمع والاعتداء الرقمي تداخلا بين السياسي والأمني والاجتماعي والديني، وبين الواقعي والافتراضي، وهو ما جعل الناشطات أكثر حذرا في سرد تجاربهن الرقمية، وفي التعبير عن مواقفهن الحقوقية في البيئات الرقمية، وصولًا إلى حذف حساباتهن من الشبكات الاجتماعية أو اقتصار نشاطهن على المتابعة واستخدامها لأغراض التسوق والتواصل مع الأصدقاء.

- وخلصت الدراسة أنه في ظل حجم القيود والمخاطر التي تعترض فلسطينيي الداخل فإن سؤال جدوى استخدام البيئة الرقمية للنضال الحقوقي والتعبير عن الرأي السياسي والاجتماعي أصبح يطرح بقوة في ضوء ارتفاع الأثمان التي يدفعها الناشطون والمستخدمون أمام تنامي خطابات الكراهية وإجراءات القمع التي تتخذها دولة إسرائيل وأجهزتها ومجموعات إسرائيلية يمينية متطرفة ضدهم.

- برز في نقاشات المجموعات البؤرية حالة من الاصطدام الجلي بين الهوية الوطنية والمواطنة، في ممارسات المشاركات والمشاركين اليومية، ولا سيما على الشبكات الرقمية وقد تفاقم هذا التصادم والتناقض بعد بدء الحرب على قطاع غزة. وقد عزز هذا التصادم شعور فقدان الأمان الرقمي، وشعور عدم الرغبة في التفاعل والنشر، أو حذف الأصدقاء أو المعارف اليهود الإسرائيليين من حسابات المشاركات والمشاركين على الشبكات الاجتماعية.

مقترحات ومساحات للعمل

أولًا، تعزيز الوعي بالأمان الرقمي

إطلاق حملات توعية مكثفة تستهدف فئات الناشطات/ين والشباب والأهالي والمعلمين، لتعريفهم بمخاطر الأمان الرقمي ووسائل الحماية الفعالة. تشمل هذه الحملات جلسات تدريب عملية وندوات في المدارس ومع الحراكات الشبابية والمجتمعات المحلية، حول استخدام الأدوات التقنية الآمنة وبرامج الحماية الحديثة وللتعريف بمبادئ وأساسيات الأمان الرقمي وتجنب الوقوع ضحية للهجمات الرقمية، وتسليط الضوء على أهمية حماية البيانات الشخصية كحق من حقوق الإنسان، وضمان استخدام الإنترنت بشكل آمن كجزء من الحق في الخصوصية وحرية التعبير.

ثانيًا، إتاحة المصادر الموثوقة للمعلومات

إنشاء وإتاحة مواد تعليمية متعددة الوسائط حول الأمان الرقمي، بما في ذلك كتيبات إرشادية، فيديوهات تعليمية، ودورات تدريبية عبر الإنترنت. يجب أن تكون هذه المواد متاحة للجميع بشكل مجاني وسهل الوصول، وأن تشمل مشاركة أفضل الممارسات للأمان الرقمي وإتاحة مصادر تشرح كيفية حماية البيانات

الشخصية والحسابات على الشبكات الاجتماعية، بما في ذلك استخدام كلمات مرور قوية، وتفعيل المصادقة الثنائية، وتشجيع استخدام أدوات الحماية المتقدمة مثل مضادات الفيروسات وجدران الحماية. عبر توفير دعم تقني مجاني للمساعدة في تهيئة واستخدام هذه الأدوات بكفاءة وتوفير إرشادات سهلة الفهم تشجع وتتيح الاستخدام الواسع النطاق لهذه الأدوات.

ثالثًا، مواجهة سياسات القمع الرقمي

توفير الدعم للناشطات/ين وتعزيز قدرتهم على مواجهة سياسات القمع الرقمي و الهجمات الرقمية، كإقامة خطوط ومنصات استشارية تقدم الدعم والتوجيه القانوني والنفسي حول الاستهداف والملاحقة الرقمية، والدعم التقني والإرشاد في مواجهة الهجمات الرقمية. إلى جانب تطوير خطط استجابة سريعة وفعالة للتعامل مع الهجمات الرقمية، بحيث تشمل هذه الخطط آليات واضحة للإبلاغ عن الحوادث وكيفية التعامل معها. ينبغي أن يتم التدريب على هذه الخطط بانتظام، ورصد الميزانيات لدعم الأبحاث المتعلقة بتوثيق ومواجهة انتهاكات الحقوق الرقمية كحقوق إنسان، لضمان جاهزية الأفراد والمؤسسات للتصدي لأي تهديد رقمي بشكل فعال.

رابعًا، توثيق الانتهاكات الرقمية

توثيق الانتهاكات الرقمية بحق الناشطات/ين الفلسطينيين و/أو المحتوى الفلسطيني والمطالبة بمحاسبة الجهات المسؤولة عنها، ونشر تقارير دورية تلخص الانتهاكات الرقمية المكتشفة وتسليط الضوء على الأنماط المتكررة والتحديات القائمة. يمكن استخدام هذه التقارير لزيادة الوعي بالانتهاكات الرقمية باعتبارها انتهاكات لحقوق الإنسان على المستويين المحلي والدولي. وتطوير دراسات وأبحاث تحليلية تربط بين هذه الانتهاكات وتأثيرها على الحقوق الأساسية مثل حرية التعبير والحق في الخصوصية. إلى جانب تدريب مجموعات متخصصة في تحليل البيانات المتعلقة بالانتهاكات الرقمية، ليكون لدى هؤلاء المتخصصين المعرفة التقنية والقانونية اللازمة للتوثيق والتحليل.

خامسًا، تعزيز التعاون مع السلطات المحلية

تعزيز الشراكات الفعالة مع لجنة المتابعة العليا واللجنة القطرية لرؤساء المجالس المحلية والحراكات السياسية، وتطوير خطة شاملة للتربية الإعلامية تشمل حرية التعبير والحقوق الرقمية وتعزيز الأمان الرقمي على المستوى المحلي. يشمل ذلك التعاون مع الجهات المعنية لتبني هذه الخطة كجزء أساسي من خطط التربية المحلية، ودمج موضوع الحقوق الرقمية ضمن حقوق الإنسان في خطط التربية الإعلامية، والتأكيد على أن تعزيز الأمان الرقمي هو جزء من حماية الأفراد وحقوقهم. ورصد ميزانيات لتطوير برامج تعليمية وورشات عمل وحملات توعية تستهدف المجتمعات المحلية لزيادة الوعي حول الحقوق الرقمية وحرية التعبير كحقوق إنسان. إضافة إلى تطوير آليات استجابة سريعة للتعامل مع الهجمات الرقمية على المستوى المحلي وتقديم الدعم والمساعدة الفورية للمتضررين.كما ينبغي الدفع بإدراج موضوعي حماية الحقوق الرقمية والأمان الرقمي ضمن المناهج الدراسية في المدارس وتطوير برامج تعليمية تزيد من وعي الطلاب بأهمية الأمان الرقمي والحقوق المرتبطة بالفضاء الرقمي، إلى جانب وضع خطط لتحسين البنية التحتية الرقمية وتوفير الأدوات التقنية اللازمة لتعزيز الأمان الرقمي، مما يسهم في توفير بيئة آمنة تدعم حرية التعبير والحقوق الرقمية.

سادسًا، تعزيز التعاون مع شركات التكنولوجيا

التعاون مع شركات التكنولوجيا لضمان الاستجابة السريعة والفعالة للتهديدات الإلكترونية على منصاتها، والعمل على تطوير آليات الرقابة على المحتوى بما يتلاءم مع اللهجات والسياق في الداخل، مع ضمان الشفافية في تعاملها مع الطلبات المتعلقة بالمحتوى الفلسطيني وضمان احترام الحقوق الرقمية للمستخدمين الفلسطينيين.

سابعًا، تقديم حلول مخصصة

إجراء الدراسات الميدانية لفهم الفروق الجندرية والثقافية في تجارب مستخدمي الإنترنت، وتسليط الضوء عليها وتطوير حلول تلبي احتياجات كل فئة بشكل يتناسب مع خصوصيتها الاجتماعية والثقافية. يتضمن ذلك تنظيم ورش عمل توعوية حول التحديات الخاصة التي تواجهها الفئات المختلفة في الفضاء الرقمي، وكيفية التصدي لها باستخدام حلول مخصصة. إلى جانب التعاون مع منظمات المجتمع المدني لتقديم الدعم اللازم للفئات المستهدفة، وضمان أن الحلول المقدمة تلبي احتياجاتهم الخاصة وتساعدهم في تحقيق الأمان الرقمي.

اتصلوا بنا:

info@7amleh.org | www.7amleh.org

Find us on social media : **7amleh**